

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号
特開2001-92721
(P2001-92721A)

(43)公開日 平成13年4月6日(2001.4.6)

(51)Int.Cl. ⁷	識別記号	F I	テ-リ-ト*(参考)
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 F 5 B 0 1 7
13/00	3 5 4	13/00	3 5 4 D 5 B 0 4 9
17/60		15/21	3 3 0 5 B 0 8 9
G 1 0 L 11/00		G 1 0 L 9/00	E 9 A 0 0 1

審査請求 未請求 請求項の数8 O L (全 38 頁)

(21)出願番号 特願平11-264616

(22)出願日 平成11年9月17日(1999.9.17)

(71)出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中4丁目1番
1号

(72)発明者 蒲田 順

神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

(72)発明者 小谷 誠剛

神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

(74)代理人 100089118

弁理士 酒井 宏明

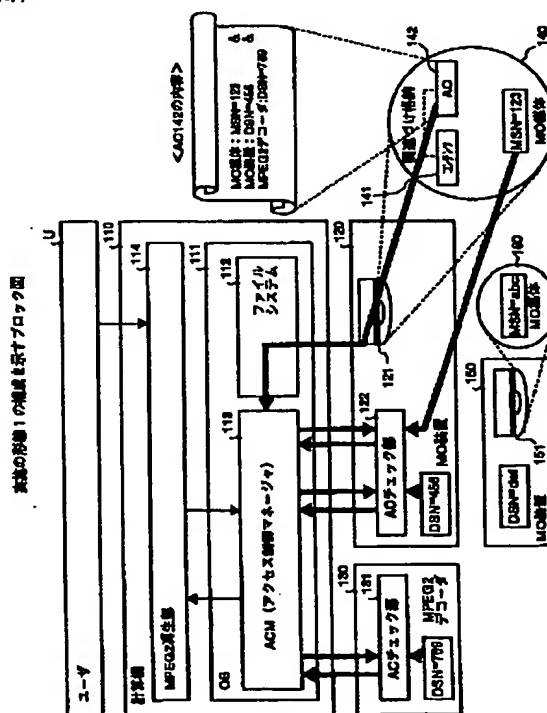
最終頁に続く

(54)【発明の名称】 コンテンツ利用制御装置、コンテンツ利用制御システムおよびコンテンツ利用制御プログラムを記録したコンピュータ読み取り可能な記録媒体

(57)【要約】

【課題】 コンテンツを容易に利用することができるとともに、コンテンツの不正利用を防止すること。

【解決手段】 コンテンツ141を利用するためのものであって、それぞれに識別情報(MSN=123、DSN=456、DSN=789)が付与されたMO装置120、MPEG2デコーダ130およびMO媒体140を備え、このMO媒体140には、コンテンツ141に関連づけられたAC(許諾情報)142が記録されており、AC142および識別情報に基づいて、コンテンツ141の利用が制御される。



【特許請求の範囲】

【請求項 1】 情報提供権限者から利用者に提供されるコンテンツの利用制御を行うコンテンツ利用制御装置において、

前記コンテンツが記録されたメディアを含み、前記コンテンツを利用するための利用手段であって、自身を構成する物理要素に関する識別情報が付与された利用手段と、

前記利用手段に付与された識別情報および前記コンテンツの利用に関する許諾情報に基づいて、前記コンテンツの利用を制御する利用制御手段とを備え、

前記メディアには、前記コンテンツに関連づけられた前記許諾情報が記録されていることを特徴とするコンテンツ利用制御装置。

【請求項 2】 前記許諾情報は、複数の物理要素に対応する複数の部分許諾情報からなり、前記メディアには、前記複数の物理要素に対応するそれぞれの識別情報で多重暗号化された前記複数の部分許諾情報が記録されており、前記利用制御手段は、前記複数の物理要素に対応するそれぞれの識別情報と、前記複数の物理要素に対応するそれぞれの識別情報を用いて前記部分許諾情報を復号した結果とに基づいて、前記コンテンツの利用を制御することを特徴とする請求項 1 に記載のコンテンツ利用制御装置。

【請求項 3】 前記メディアには、暗号化されたコンテンツが記録されているとともに、前記複数の部分許諾情報および前記コンテンツを復号するためのコンテンツ復号鍵が多重暗号化されたものが記録されており、前記利用手段は、前記利用制御手段により利用が許諾された場合に、前記コンテンツ復号鍵を用いて前記コンテンツを復号した結果に基づいてコンテンツを利用することを特徴とする請求項 2 に記載のコンテンツ利用制御装置。

【請求項 4】 前記メディアは、暗号化された情報が記録されるセキュア領域を有しており、前記セキュア領域には、暗号化された前記許諾情報が記録されており、前記利用制御手段は、前記セキュア領域に記録された前記許諾情報の復号結果および前記識別情報に基づいて、前記コンテンツの利用を制御することを特徴とする請求項 1 に記載のコンテンツ利用制御装置。

【請求項 5】 前記利用手段は、少なくとも二つの物理要素で構成され、前記二つの物理要素は、相互認証コマンドが発行された際に相互認証を行い、前記メディアは、前記相互認証コマンドが発行されかつ前記相互認証がとられた場合にのみアクセス可能な特別領域を有しており、前記特別領域には、前記許諾情報が格納されており、前記利用制御手段は、前記相互認証コマンドが発行されかつ前記相互認証がとられた場合にのみ、前記特別領域から前記許諾情報を取得し、該許諾情報および前記識別情報に基づいて、前記コンテンツの利用を制御することを特徴とする請求項 1 に記載のコンテンツ利用制御

装置。

【請求項 6】 前記特別領域は、暗号化された情報が記録されるセキュア領域とマッピングされていることを特徴とする請求項 5 に記載のコンテンツ利用制御装置。

【請求項 7】 情報提供権限者から利用者に提供されるコンテンツと、前記コンテンツの利用に関する許諾情報とが関連付けられて記録されたメディアから、前記コンテンツおよび前記許諾情報を読み出す読出手段と、読み出された前記コンテンツと前記許諾情報とを一つのファイルとして転送する転送手段と、前記一つのファイルを受信する受信手段と、前記受信手段により受信された前記一つのファイルから前記コンテンツおよび前記許諾情報を生成し、これらを別のメディアに書き込む書込手段とを備えることを特徴とするコンテンツ利用制御システム。

【請求項 8】 情報提供権限者から利用者に提供されるコンテンツが記録されたメディアを含み、前記コンテンツを利用するための利用手段であって、自身を構成する物理要素に関する識別情報が付与された利用手段を備えるコンテンツ利用制御装置に適用されるコンテンツ利用制御プログラムを記録したコンピュータ読み取り可能な記録媒体であって、前記メディアには、前記コンテンツに関連づけられた前記許諾情報が記録されており、前記利用手段に付与された識別情報および前記コンテンツの利用に関する許諾情報に基づいて、前記コンテンツの利用を制御させる利用制御工程をコンピュータに実行させるための利用制御プログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】**【0001】**

【発明の属する技術分野】本発明は、著作権者等の情報提供権限者により提供されるコンテンツの利用に関する制御を行うコンテンツ利用制御装置、コンテンツ利用制御システムおよびコンテンツ利用制御プログラムを記録したコンピュータ読み取り可能な記録媒体に関するものである。

【0002】近時においては、デジタル化された映画、音楽等のコンテンツの配信が本格的にスタートしたことから、この種のコンテンツに関する著作権、許諾を管理する機構の実現が急がれている。

【0003】

【従来の技術】従来より、映画、音楽等のコンテンツ（著作物）に関しては、著作権者の許諾を得なければ、営利目的で販売、譲渡することができない。ここでいうコンテンツは、単一の記録媒体に記録可能なビット列の集合としての構造をもつデジタルコンテンツであり、文章テキスト、静止画、動画、プログラムソフトウェア等をいう。

【0004】この種のコンテンツは、記録媒体に記録さ

れた状態で利用者に配布される。この場合、著作権保護を目的として、許諾情報を用いたコンテンツの利用に関する制御（以下、コンテンツ利用制御という）が行われる。このコンテンツ利用制御は、正当な許諾を受けた利用者のみがコンテンツを利用できるようにするためのものである。

【0005】たとえば、コンテンツ利用制御の一例としては、コンテンツを利用する上で必要な物理要素（システム（記録媒体、装置））を特定するための識別情報からなる許諾情報を利用するものがある。この許諾情報には、コンテンツの利用に関する許諾条件が含まれている。上記システムには、固有の識別情報が付与されている。この場合、利用者は、コンテンツの入手経路とは別の経路から上記許諾情報を入手する。つぎに、利用者は、上記許諾情報をシステムに入力した後、このシステムにコンテンツが記録された記録媒体をセットする。

【0006】これにより、システムは、自身に付与されている識別情報が、利用者により入力された許諾情報に含まれる許諾条件を満たしているか否かを判断する。ここで、許諾条件を満たしている場合には、コンテンツの利用が許諾される。一方、許諾条件を満たしていない場合には、コンテンツの利用が許諾されない。

【0007】

【発明が解決しようとする課題】ところで、前述したように、従来においては、コンテンツを利用する場合、コンテンツが記録された記録媒体と、許諾情報とを別々の経路から入手しなければならないため、非常に不便である。また、従来においては、記録媒体と許諾情報とが別になっているため、一方を紛失する可能性がある。

【0008】さらに、従来においては、許諾情報のみが単体で存在しているため、許諾情報の不正コピーが可能であり、この結果、コンテンツが不正利用されるという問題があった。これは、著作権者保護の観点から許容されるものではない。

【0009】本発明は、上記に鑑みてなされたもので、コンテンツを容易に利用することができ、コンテンツの不正利用を防止することができるコンテンツ利用制御装置、コンテンツ利用制御システムおよびコンテンツ利用制御プログラムを記録したコンピュータ読み取り可能な記録媒体を提供することを目的とする。

【0010】上記目的を達成するために、請求項1にかかる発明は、情報提供権限者から利用者に提供されるコンテンツの利用制御を行うコンテンツ利用制御装置において、前記コンテンツが記録されたメディア（後述する実施の形態1のMO媒体140に相当）を含み、前記コンテンツを利用するための利用手段であって、自身を構成する物理要素に関する識別情報が付与された利用手段（後述する実施の形態1のMO装置120、MPEG2デコーダ130、MO媒体140に相当）と、前記利用手段に付与された識別情報および前記コンテンツの利用

に関する許諾情報に基づいて、前記コンテンツの利用を制御する利用制御手段（後述する実施の形態1の計算機110に相当）とを備え、前記メディアには、前記コンテンツに関連づけられた前記許諾情報が記録されていることを特徴とする。

【0011】この請求項1にかかる発明によれば、利用制御手段は、メディアから取得した許諾情報と識別情報とに基づいて、コンテンツの利用を制御する。ここで、利用が許諾された場合には、利用手段は、メディアからコンテンツを取得した後、これを利用する。

【0012】このように、請求項1にかかる発明によれば、許諾情報とコンテンツとを関連付けて一つのメディアに記録し、この許諾情報および識別情報に基づいて、コンテンツの利用の制御を行うようにしたので、一つのメディアを入手することで同時に許諾情報とコンテンツとが得られるため、許諾情報とコンテンツとを別々に入手していた従来に比して、コンテンツを容易に利用することができる。

【0013】また、請求項2にかかる発明は、請求項1に記載のコンテンツ利用制御装置において、前記許諾情報は、複数の物理要素に対応する複数の部分許諾情報からなり、前記メディア（後述する実施の形態2のMO媒体240に相当）には、前記複数の物理要素に対応するそれぞれの識別情報で多重暗号化された前記複数の部分許諾情報が記録されており、前記利用制御手段（後述する実施の形態2の計算機210に相当）は、前記複数の物理要素に対応するそれぞれの識別情報と、前記複数の物理要素に対応するそれぞれの識別情報を用いて、前記部分許諾情報を復号した結果とに基づいて、前記コンテンツの利用を制御することを特徴とする。

【0014】この請求項2にかかる発明によれば、利用制御手段は、メディアから取得した部分許諾情報を復号し、この復号結果と識別情報とに基づいて、コンテンツの利用を制御する。ここで、部分許諾情報をすべて復号できるのは、正当な許諾を受ける権限を有する利用者に属する装置である。したがって、部分許諾情報を復号できなかった場合には、当該装置は、不正利用者に属していることになる。

【0015】このように請求項2にかかる発明によれば、複数の部分許諾情報を多重暗号化してメディアに記録するようにしたので、コンテンツの不正利用を防止することができる。

【0016】また、請求項3にかかる発明は、請求項2に記載のコンテンツ利用制御装置において、前記メディア（後述する実施の形態3のMO媒体240に相当）には、暗号化されたコンテンツが記録されているとともに、前記複数の部分許諾情報および前記コンテンツを復号するためのコンテンツ復号鍵が多重暗号化されたものが記録されており、前記利用手段は、前記利用制御手段により利用が許諾された場合に、前記コンテンツ復号鍵

を用いて前記コンテンツを復号した結果に基づいてコンテンツを利用することを特徴とする。

【0017】この請求項3にかかる発明によれば、利用制御手段は、メディアから取得した部分許諾情報を復号し、この復号結果と識別情報とに基づいて、コンテンツの利用を制御する。ここで、部分許諾情報およびコンテンツ復号鍵をすべて復号できるのは、正当な許諾を受ける権限を有する利用者に属する装置である。さらに、利用手段は、利用制御手段により利用が許諾された場合に、コンテンツ復号鍵を用いてコンテンツを復号した結果に基づいてコンテンツを利用する。

【0018】このように請求項3にかかる発明によれば、複数の部分許諾情報に加えてコンテンツを復号するためのコンテンツ復号鍵を多重暗号化してメディアに記録するようにしたので、コンテンツの不正利用をより効果的に防止することができる。

【0019】また、請求項4にかかる発明は、請求項1に記載のコンテンツ利用制御装置において、前記メディア（後述する実施の形態4のMO媒体440に相当）は、暗号化された情報が記録されるセキュア領域を有しており、前記セキュア領域には、暗号化された前記許諾情報が記録されており、前記利用制御手段は、前記セキュア領域に記録された前記許諾情報の復号結果および前記識別情報に基づいて、前記コンテンツの利用を制御することを特徴とする。

【0020】この請求項4にかかる発明によれば、利用制御手段は、セキュア領域に記録された許諾情報の復号結果および識別情報に基づいて、コンテンツの利用を制御する。ここで、許諾情報を復号できるのは、正当な許諾を受ける権限を有する利用者に属する装置である。したがって、許諾情報を復号できなかった場合には、当該装置は、不正利用者に属していることになる。

【0021】このように請求項4にかかる発明によれば、メディアのセキュア領域に暗号化された許諾情報を記録するようにしたので、コンテンツの不正利用を防止することができる。

【0022】また、請求項5にかかる発明は、請求項1に記載のコンテンツ利用制御装置において、前記利用手段（後述する実施の形態5のファイルシステム510およびMO装置520に相当）は、少なくとも二つの物理要素で構成され、前記二つの物理要素は、相互認証コマンドが発行された際に相互認証を行い、前記メディア（後述する実施の形態5の540に相当）は、前記相互認証コマンドが発行されかつ前記相互認証がとられた場合にのみアクセス可能な特別領域を有しており、前記特別領域には、前記許諾情報が格納されており、前記利用制御手段は、前記相互認証コマンドが発行されかつ前記相互認証がとられた場合にのみ、前記特別領域から前記許諾情報を取得し、該許諾情報および前記識別情報に基づいて、前記コンテンツの利用を制御することを特徴と

する。

【0023】この請求項5にかかる発明によれば、相互認証コマンドが発行されると、二つの物理要素は、相互認証を行う。ここで、相互認証がとられた場合には、利用制御手段は、特別領域から許諾情報を取得し、該許諾情報および識別情報に基づいて、コンテンツの利用を制御する。一方、相互認証がとられなかった場合には、許諾が与えられない。

【0024】このように、請求項5にかかる発明によれば、メディアの特別領域に許諾情報を記録し、二つの物理要素間で相互認証がとられた場合にのみ、該特別領域から許諾情報を取得するようにしたので、相互認証がとられない場合に、即時に許諾不可とすることができ、コンテンツの不正利用を防止することができる。

【0025】また、請求項6にかかる発明は、請求項5に記載のコンテンツ利用制御装置において、前記特別領域（後述する実施の形態6の特別領域B₂に相当）は、暗号化された情報が記録されるセキュア領域とマッピングされていることを特徴とする。

【0026】この請求項6にかかる発明によれば、いずれもセキュリティ上有効である特別領域にセキュア領域をマッピングするようにしたので、極めて高いセキュリティを確保することができる。

【0027】また、請求項7にかかる発明は、情報提供権限者から利用者に提供されるコンテンツと、前記コンテンツの利用に関する許諾情報とが関連付けられて記録されたメディアから、前記コンテンツおよび前記許諾情報を読み出す読出手段（後述する実施の形態7のファイルシステム822に相当）と、読み出された前記コンテンツと前記許諾情報とを一つのファイルとして転送する転送手段（後述する実施の形態7の転送部824に相当）と、前記一つのファイルを受信する受信手段（後述する実施の形態7の受信部924に相当）と、前記受信手段により受信された前記一つのファイルから前記コンテンツおよび前記許諾情報を生成し、これらを別のメディアに書き込む書込手段（後述する実施の形態7のファイルシステム922に相当）とを備えることを特徴とする。

【0028】この請求項7にかかる発明によれば、読出手段によりメディアからコンテンツおよび許諾情報が読み出されると、転送手段によりコンテンツおよび許諾情報が一つのファイルとして転送される。そして、受信手段により、上記一つのファイルからコンテンツおよび許諾情報が生成される。書込手段は、コンテンツおよび許諾情報を別のメディアに書き込む。

【0029】このように、請求項7にかかる発明によれば、一方のメディアから他方のメディアへコンテンツおよび許諾情報が転送（コピー）されるので、コンテンツの利用に関する許諾（ライセンス）を第三者に譲渡することができる。

【0030】また、請求項8にかかる発明は、情報提供権限者から利用者に提供されるコンテンツが記録されたメディアを含み、前記コンテンツを利用するための利用手段であって、自身を構成する物理要素に関する識別情報が付与された利用手段を備えるコンテンツ利用制御装置に適用されるコンテンツ利用制御プログラムを記録したコンピュータ読み取り可能な記録媒体であって、前記メディアには、前記コンテンツに関連づけられた前記許諾情報が記録されており、前記利用手段に付与された識別情報および前記コンテンツの利用に関する許諾情報に基づいて、前記コンテンツの利用を制御させる利用制御工程（後述する実施の形態1のステップSA1～ステップSA18に相当）をコンピュータに実行させるための利用制御プログラムを記録したコンピュータ読み取り可能な記録媒体である。

【0031】この請求項8にかかる発明によれば、利用制御工程では、メディアから取得した許諾情報と識別情報とに基づいて、コンテンツの利用が制御される。ここで、利用が許諾された場合には、利用手段は、メディアからコンテンツを取得した後、これを利用する。

【0032】このように、請求項8にかかる発明によれば、許諾情報とコンテンツとを関連付けて一つのメディアに記録し、これらの許諾情報および識別情報に基づいて、コンテンツの利用の制御を行うようにしたので、一つのメディアを入手することで同時に許諾情報とコンテンツとが得られるため、許諾情報とコンテンツとを別々に入手していた従来に比して、コンテンツを容易に利用することができる。

【0033】

【発明の実施の形態】以下、図面を参照して本発明にかかるコンテンツ利用制御装置、コンテンツ利用制御システムおよびコンテンツ利用制御プログラムを記録したコンピュータ読み取り可能な記録媒体の実施の形態1～8について詳細に説明する。

【0034】（実施の形態1）図1は、本発明にかかる実施の形態1の構成を示すブロック図である。この図において、計算機110は、ユーザUにより操作されるものであり、OS（Operating System）111を備えている。この計算機110においては、OS111により各種プログラムの実行が制御される。ファイルシステム112は、計算機110で扱われるファイルを管理し、データのリード/ライトを制御する。ACM（Access Control Manager：アクセス制御マネージャ）113は、ファイルシステム112、MPEG2（Moving Picture Experts Group 2）再生部114、MO（Magnet Optic）装置120、MPEG2デコーダ130相互間のアクセス制御を管理する。

【0035】MPEG2再生部114は、後述するMPEG2デコーダ130へ動画データ（コンテンツ）を供給する等の制御を行う。実際には、MPEG2再生部1

14の機能は、MPEG2再生アプリケーションプログラム（図示略）が実行されることにより実現される。MO装置120は、計算機110に外付け（または内蔵）されており、MO媒体（同図の場合、MO媒体140）からデータを読み取る。

【0036】このMO媒体140には、コンテンツ141とAC（Access Condition：アクセス許可条件を示す情報）142とが関連付けられた状態で格納されている。このコンテンツ141は、たとえば、MPEG2方式の動画データであり、著作権者等の情報提供権限者により提供される。なお、コンテンツ141としては、著作権、許諾に関わるものであればそのデータ形式は問わない。AC142は、コンテンツ141の再生に関する許諾情報である。つまり、AC142の条件を満たす場合には、コンテンツ141の再生が許諾され、一方、AC142の条件を満たさない場合には、コンテンツ141の再生が許諾されない。

【0037】ここで、AC142の条件は、複数の対象物理要素にそれぞれ付与された識別情報の組み合わせからなる。この対象物理要素としては、コンテンツ141を再生するために必要な装置、媒体であり、MO媒体、MO装置、MPEG2装置である。また、識別情報としては、MSN（Media Serial Number：媒体シリアル番号）、DSN（Device Serial Number：装置シリアル番号）である。具体的には、AC142においては、MO媒体のMSNが「123」、MO装置のDSNが「456」、MPEG2デコーダのDSNが「789」に設定されている。また、AC142においては、MSN（＝123）&DSN（＝456）&DSN（＝789）という論理積（アンド）条件が設定されている。

【0038】つまり、AC142によれば、MSN（＝123）が付与されたMO媒体であること、MSN（＝456）が付与されたMO装置であること、DSN（＝789）が付与されたMPEG2デコーダであること、という三つの条件がすべて満たされた場合にのみ、コンテンツ141の再生が許諾される。逆に言えば、上記三つの条件のうち一つまたは二つの条件が満たされない場合には、コンテンツ141の再生が許諾されない。つまり、AC142は、上記三つの条件を同時に満たすことができる正当な者に対してのみコンテンツ141の再生を許諾させるライセンスとしての役目をしている。

【0039】また、コンテンツ141とAC142は、図2に示したように関連づけられた状態でMO媒体140に格納されている。MO媒体140において、コンテンツ141は、コンテンツ（1/3）141₁、コンテンツ（2/3）141₂、コンテンツ（3/3）141₃という具合に三分割されている。これらのコンテンツ（1/3）141₁、コンテンツ（2/3）141₂、コンテンツ（3/3）141₃は、LBN（Logical Block Number：論理ブロック番号）＝L、LBN＝Mおよび

びLBN=Nでそれぞれ指定された領域に格納されている。

【0040】同様に、MO媒体140において、AC142は、AC(1/2)142₁、AC(2/2)142₂という具合に二分割されている。これらのAC(1/2)142₁、AC(2/2)142₂は、LBN=X、LBN=Yでそれぞれ指定された領域に格納されている。

【0041】また、コンテンツ141とAC142とは、ファイル管理データD_{A1}および補助ファイル管理データD_{A2}を介して関連付けられている。ファイル管理データD_{A1}は、ファイル本体としてのコンテンツ141および補助ファイルとしてのAC142を管理するためのデータである。このファイル管理データD_{A1}は、「ファイル名」、「作成日時」、…「補助ファイル管理データへのリンク」、「ファイル本体へのリンク(1/3)」、「ファイル本体へのリンク(2/3)」および「ファイル本体へのリンク(3/3)」という情報から構成されている。

【0042】一方、補助ファイル管理データD_{A2}は、AC142を直接、管理するためのデータであり、「補助ファイル名」、「作成日時」、…「ACへのリンク(1/2)」、「ACへのリンク(2/2)」という情報から構成されている。

【0043】図3は、AC142(図1参照)のフォーマットの一例を示す図である。この図において、フラグF₄は、MO媒体AC:MSN=123(図1参照)が論理和(オア)/論理積条件(アンド条件)でないことを示すものである。フラグF₅は、MO装置AC:DSN=456(図1参照)が論理和/論理積条件でないことを示すものである。フラグF₃は、上記MO媒体AC:MSN=123とMO装置AC:DSN=456とが論理和条件であることを示すものである。この場合、論理和条件の個数は2である。

【0044】フラグF₆は、MPEG2デコードAC:DSN=789が論理和/論理積条件でないことを示すものである。フラグF₂は、フラグF₃に関する要素(MSN=123、DSN=456)と、フラグF₆に関する要素(DSN=789)とが論理和条件であることを示すものである。この場合、論理和条件の個数は2である。ここで、図1に示したAC142においては、上述したフラグF₂からフラグF₆までのフォーマットが用いられている。したがって、図3に示したフラグF₁、フラグF₇～フラグF₉は、拡張用である。

【0045】フラグF₈は、MO媒体AC:MSN=a b cが論理和/論理積条件でないことを示すものである。フラグF₉は、MO装置AC:DSN=d e fが論理和/論理積条件でないことを示すものである。フラグF₇は、フラグF₈に関する要素(MSN=a b c)とフラグF₉に関する要素(DSN=d e f)とが論理積

条件であることを示すものである。この場合の論理積条件の個数は2である。フラグF₁は、フラグF₂に関する要素(MSN=123、DSN=456、DSN=789)と、フラグF₇に関する要素(MSN=a b c、DSN=d e f)とが論理和条件であることを示すものである。この場合、論理和条件の個数は2である。

【0046】図1に戻り、MO媒体140には、自身の識別情報であるMSN=123が付与されている。MO装置120には、自身の識別情報であるDSN=456が付与されている。ドライブ121は、データ読み出し時にMO媒体140を回転駆動する。ACチェック部122は、MO媒体140から読み出されたMSN=123が、AC142の条件(この場合、MSN=123)を満たすか否かをチェックする。同様に、ACチェック部122は、MO装置120に付与されたDSN=456が、AC142の条件(この場合、DSN=456)を満たすか否かをチェックする。

【0047】MPEG2デコード130は、MPEG2方式によりコンテンツ141(動画データ)をデコードすることにより、コンテンツ141を再生する。このMPEG2デコード130には、自身の識別情報であるDSN=789が付与されている。ACチェック部131は、AC142の条件(この場合、DSN=789)を満たすか否かをチェックする。

【0048】MO装置150は、MO装置120に対して別設(または併設)されており、MO媒体(同図の場合、MO媒体160)からデータを読み出す。このMO装置150において、ドライブ151は、MO媒体160を回転駆動する。また、MO装置150には、自身の識別情報であるDSN=d e f(図3参照)が付与されている。このDSN=d e fは、MO装置120に付与されたDSN=456と異なる。MO媒体160には、自身の識別情報であるMSN=a b cが付与されている。このMSN=a b cは、MO媒体140に付与されているMSN=123と異なる。

【0049】つぎに、上述した実施の形態1の動作について図4に示したフローチャートを参照しつつ説明する。この場合、図1に示したMO装置120のドライブ121には、MO媒体140がセットされているものとする。この状態において、図4に示したステップSA1でユーザUからMPEG2再生部114に対してMPEG2(コンテンツ)の再生が指示されると、ステップSA2では、MPEG2再生部114は、ACM113に対してMPEG2(コンテンツ)の再生を指示する。

【0050】これにより、ステップSA3では、ACM113は、MO媒体140から、ファイルシステム112経由でAC142を取得した後、ステップSA4へ進む。ステップSA4では、ACM113は、取得したAC142をMO装置120のACチェック部122へ転送する。これにより、ステップSA5では、ACチェッ

ク部122は、MO媒体140からMSN (=123)を取得した後、ステップSA6へ進む。ステップSA6では、ACチェック部122は、AC142の条件とMSN (=123)とが一致するか否かを判断する。

【0051】具体的には、ACチェック部122は、図1に示したAC142の内容(この場合、MO媒体:MSN=123)とMO媒体140から取得したMSN (=123)とが一致するか否かを判断する。この場合、両者が一致するため、ACチェック部122は、ステップSA6の判断結果を「Yes」として、ステップSA7へ進む。

【0052】一方、ステップSA6の判断結果が「No」である場合、すなわち、両者が一致しない場合、ACチェック部122は、ステップSA17へ進む。ステップSA17では、ACチェック部122は、ACM113にチェック結果=NGを返答する。これにより、ステップSA18では、ACM113は、MPEG2再生部114にチェック結果=NGを返答した後、一連の処理を終了する。つまり、この場合には、AC142の条件(MSN=123)が満たされていないため、MO媒体140に記録されたコンテンツ141の再生が許諾されない。

【0053】この場合、ステップSA7では、ACチェック部122は、ACM113に対してステップSA6におけるチェック結果=OKとともに、AC142を返却する。これにより、ステップSA8では、ACM113は、ACチェック部122にAC142を転送する。そして、上記AC142を受信すると、ステップSA9では、ACチェック部122は、MO装置120よりDSN (=456)を取得した後、ステップSA10へ進む。ステップSA10では、ACチェック部122は、AC142の条件とDSN (=456)とが一致するか否かを判断する。

【0054】具体的には、ACチェック部122は、図1に示したAC142の内容(この場合、MO装置:DSN=456)とMO装置120から取得したDSN (=456)とが一致するか否かを判断する。この場合、ACチェック部122は、両者が一致するため、ステップSA10の判断結果を「Yes」として、ステップSA11へ進む。

【0055】一方、ステップSA10の判断結果が「No」である場合、言い換えれば、両者が一致しない場合、ACチェック部122は、ステップSA17へ進む。ステップSA17では、ACチェック部122は、ACM113にチェック結果=NGを返答する。これにより、ステップSA18では、ACM113は、MPEG2再生部114にチェック結果=NGを返答した後、一連の処理を終了する。つまり、この場合には、AC142の条件(MSN=123&DSN=456)が満たされていないため、MO媒体140に記録されたコンテ

ンツ141の再生が許諾されない。

【0056】この場合、ステップSA11では、ACチェック部122は、ACM113に対して、ステップSA10におけるチェック結果=OKとともにAC142を返却する。これにより、ステップSA12では、ACM113は、MPEG2デコーダ130のACチェック部131へAC142を転送する。そして、上記AC142を受信すると、ステップSA13では、ACチェック部131は、MPEG2デコーダ130よりDSN (=789)を取得した後、ステップSA14へ進む。ステップSA14では、ACチェック部131は、AC142の条件とDSN (=789)とが一致するか否かを判断する。

【0057】具体的には、ACチェック部131は、図1に示したAC142の内容(この場合、MPEG2デコーダ:DSN=789)とMPEG2デコーダ130から取得したDSN (=789)とが一致するか否かを判断する。この場合、ACチェック部131は、両者が一致するため、ステップSA14の判断結果を「Yes」として、ステップSA15へ進む。

【0058】一方、ステップSA14の判断結果が「No」である場合、言い換えれば、両者が一致しない場合、ACチェック部131は、ステップSA17へ進む。ステップSA17では、ACチェック部131は、ACM113にチェック結果=NGを返答する。これにより、ステップSA18では、ACM113は、MPEG2再生部114にチェック結果=NGを返答した後、一連の処理を終了する。つまり、この場合には、AC142の条件(MSN=123&DSN=456&DSN=789)が満たされていないため、MO媒体140に記録されたコンテンツ141の再生が許諾されない。

【0059】この場合、ステップSA15では、ACチェック部131は、ステップSA14のチェック結果=OKとともにAC142をACM113に返却する。これにより、ステップSA16では、ACM113は、MPEG2再生部114に対して、ステップSA6、ステップSA10およびステップSA14のすべてのチェック結果=OKを返答した後、一連の処理を終了する。つまり、この場合には、MO媒体140に記録されたAC142の条件がすべて満たされているため、MO媒体140に記録されたコンテンツ141の再生が許諾される。

【0060】したがって、MPEG2再生部114は、ドライブ121およびファイルシステム112を経由してMO媒体140からコンテンツ141を読み出した後、これをMPEG2デコーダ130へ転送する。これにより、MPEG2デコーダ130においては、コンテンツ141が動画再生される。

【0061】以上説明したように、実施の形態1によれば、AC142とコンテンツ141とを関連付けて一つ

のMO媒体140に記録し、AC142および識別情報(MSN=123等)に基づいて、コンテンツ141の利用の制御を行うようにしたので、MO媒体140を入手することで同時にAC142とコンテンツ141とが得られるため、別々に入手していた従来に比して、コンテンツを容易に利用することができる。

【0062】(実施の形態2)さて、前述した実施の形態1においては、図1に示したAC142に対して特に暗号化の処理を施していない例について説明したが、AC142を暗号化することによりセキュリティを高めるようにしてもよい。以下においては、この場合を実施の形態2として説明する。

【0063】図5は、本発明にかかる実施の形態2の構成を示すブロック図である。この図において、計算機210は、ユーザUにより操作されるものであり、OS211を備えている。この計算機210においては、OS211により各種プログラムの実行が制御される。ファイルシステム212は、計算機210で扱われるファイルを管理し、データのリード/ライトを制御する。ACM(アクセス制御マネージャ)213は、ファイルシステム212、MPEG2再生部214、MO装置220、MPEG2デコーダ230相互間のアクセス制御を管理する。

【0064】MPEG2再生部214は、前述したMPEG2再生部114(図1参照)と同様の機能を備えている。MO装置220は、計算機210に外付け(または内蔵)されており、MO媒体(同図の場合、MO媒体240)からデータを読み取る。

【0065】このMO媒体240には、コンテンツ241と許諾情報242とが関連付けられた状態で格納されている。このコンテンツ241は、MPEG2方式の動画データである。許諾情報242は、コンテンツ241の再生の許諾に関する情報である。つまり、許諾情報242の条件を満たす場合には、コンテンツ241の再生が許諾され、一方、許諾情報242の条件を満たさない場合には、コンテンツ241の再生が許諾されない。この許諾情報242は、複数の情報(MSN=123、DSN=456およびDSN=789)が複数の暗号鍵により多重暗号化されてなる。この許諾情報242のデータ構造の詳細については図7を参照して後述する。

【0066】ここで、許諾情報242の条件は、複数の対象物理要素にそれぞれ付与された識別情報の組み合わせからなる。この対象物理要素としては、コンテンツ241を再生するために必要な装置、媒体であり、MO媒体、MO装置、MPEG2装置である。また、識別情報としては、MSN(媒体シリアル番号)、DSN(装置シリアル番号)である。具体的には、許諾情報242においては、MO媒体のMSNが「123」、MO装置のDSNが「456」、MPEG2デコーダのDSNが「789」に設定されている。また、許諾情報242に

おいては、MSN(=123)&DSN(=456)&DSN(=789)という論理積(アンド)条件が設定されている。

【0067】つまり、許諾情報242によれば、MSN(=123)が付与されたMO媒体であること、MSN(=456)が付与されたMO装置であること、DSN(=789)が付与されたMPEG2デコーダであること、という三つの条件がすべて満たされた場合にのみ、コンテンツ241の再生が許諾される。逆に言えば、上記三つの条件のうち一つまたは二つの条件が満たされない場合には、コンテンツ241の再生が許諾されない。つまり、許諾情報242は、上記三つの条件を同時に満たすことができる正当な者に対してのみコンテンツ241の再生を許諾させるライセンスとしての役目をしている。

【0068】また、コンテンツ241と許諾情報242は、前述した図2と同様に、図6に示したように関連づけられた状態でMO媒体240に格納されている。MO媒体240において、コンテンツ241は、コンテンツ(1/3)241₁、コンテンツ(2/3)241₂、コンテンツ(3/3)241₃という具合に三分割されている。これらのコンテンツ(1/3)241₁、コンテンツ(2/3)241₂、コンテンツ(3/3)241₃は、LBN=L、LBN=MおよびLBN=Nでそれぞれ指定された領域に格納されている。

【0069】同様に、MO媒体240において、許諾情報242は、許諾情報(1/2)242₁、許諾情報(2/2)242₂という具合に二分割されている。これらの許諾情報(1/2)242₁、許諾情報(2/2)242₂は、LBN=X、LBN=Yでそれぞれ指定された領域に格納されている。

【0070】また、コンテンツ241と許諾情報242とは、ファイル管理データDB₁および補助ファイル管理データDB₂を介して関連付けられている。ファイル管理データDB₁は、ファイル本体としてのコンテンツ241および補助ファイルとしての許諾情報242を管理するためのデータである。このファイル管理データDB₁は、「ファイル名」、…、「ファイル本体へのリンク(3/3)」という情報から構成されている。一方、補助ファイル管理データDB₂は、許諾情報242を直接、管理するためのデータであり、「補助ファイル名」、…、「許諾情報へのリンク(1/2)」、「許諾情報へのリンク(2/2)」という情報から構成されている。

【0071】図5に戻り、MO媒体240には、自身の識別情報であるMSN=123が付与されている。また、MO媒体240には、鍵Key=a b cが格納されている。この鍵Key=a b cは、許諾情報242からMSN=123を復号するためのものである。MO装置220には、自身の識別情報であるDSN=456が付

与されている。また、MO装置220には、鍵Key=defが格納されている。この鍵Key=defは、許諾情報242からDSN=456を復号するためのものである。

【0072】ドライブ221は、データ読み出し時にMO媒体240を回転駆動する。復号部223は、MO媒体240に格納されている鍵Key=abcを用いて、許諾情報242からMSN=123を復号する。さらに、復号部223は、MO装置220に格納されている復号鍵Key=defを用いて、許諾情報242からDSN=456を復号する。

【0073】ACチェック部222は、MO媒体240から読み出されたMSN=123が、許諾情報242の条件（この場合、MSN=123）を満たすか否かをチェックする。同様にして、ACチェック部222は、MO装置220に付与されたDSN=456が、許諾情報242の条件（この場合、DSN=456）を満たすか否かをチェックする。

【0074】MPEG2デコーダ230は、MPEG2方式によりコンテンツ241（動画データ）をデコードすることにより、コンテンツ241を再生する。このMPEG2デコーダ230には、自身の識別情報であるDSN=789が付与されている。復号部232は、MPEG2デコーダ230に格納されている鍵Key=ghiを用いて、許諾情報242からDSN=789を復号する。ACチェック部231は、許諾情報242の条件（この場合、DSN=789）を満たすか否かをチェックする。

【0075】図7は、実施の形態2におけるライセンス（許諾情報242）の一例を示す図である。この図において、MPEG2デコーダAC:DSN=789は、前述した対象物理要素としてのMPEG2デコーダに対応するものであり、鍵Key=ghiにより暗号化されている。また、DSN=789は、MPEG2デコーダ230（図5参照）にのつての許諾情報である。

【0076】MO装置AC:DSN=456は、対象物理要素としてのMO装置に対応するものである。このDSN=456と暗号化されたDSN=789とは、鍵Key=defにより多重暗号化されている。この多重暗号化されたDSN=456およびDSN=789は、MO装置220（図5参照）にのつての許諾情報である。また、MO媒体AC:MSN=123は、対象物理要素としてのMO媒体に対応するものである。このMSN=123と多重暗号化されたDSN=456およびDSN=789とは、鍵Key=abcにより多重暗号化されている。この多重暗号化されたMSN=123、DSN=456およびDSN=789は、MO媒体240（図5参照）にのつての許諾情報である。

【0077】つぎに、上述した実施の形態2の動作について図9に示したフローチャートを参照しつつ説明す

る。この場合、図5に示したMO装置220のドライブ221には、MO媒体240がセットされているものとする。この状態において、図9に示したステップSB1でユーザUからMPEG2再生部214に対してMPEG2（コンテンツ）の再生が指示されると、ステップSB2では、MPEG2再生部214は、ACM213に対してMPEG2（コンテンツ）の再生を指示する。

【0078】これにより、ステップSB3では、ACM213は、MO媒体240から、ファイルシステム212経由で暗号化された図8（a）に示した許諾情報242を取得した後、ステップSB4へ進む。ステップSB4では、ACM213は、取得した許諾情報242（図8（a）参照）をMO装置220の復号部223へ転送する。これにより、ステップSB5では、復号部223は、MO媒体240から鍵Key（=abc=K1（図8（a）参照））を取得した後、ステップSB6へ進む。

【0079】ステップSB6では、復号部223は、鍵Key（=abc=K1（図8（a）参照））を用いて許諾情報242を図8（b）に示したように復号した後、ステップSB7へ進む。ここでは、図8（b）に示したようにMSN（=123）が復号される。ステップSB7では、復号部223は、復号された許諾情報242をACチェック部222へ転送する。

【0080】これにより、ステップSB8では、ACチェック部222は、MO媒体240からMSN（=123）を取得した後、ステップSB9へ進む。ステップSB9では、ACチェック部222は、復号された図8（b）に示した許諾情報242の条件（MSN=123）と上記MSN（=123）とが一致するか否かを判断する。この場合、両者が一致するため、ACチェック部222は、ステップSB9の判断結果を「Yes」として、ステップSB10へ進む。

【0081】一方、ステップSB9の判断結果が「No」である場合、すなわち、両者が一致しない場合、ACチェック部222は、ステップSB26へ進む。ステップSB26では、ACチェック部222は、ACM213にチェック結果=NGを返答する。これにより、ステップSB27では、ACM213は、MPEG2再生部214にチェック結果=NGを返答した後、一連の処理を終了する。つまり、この場合には、許諾情報242に基づく許諾条件（MSN=123）が満たされていないため、MO媒体240に記録されたコンテンツ241の再生が許諾されない。

【0082】この場合、ステップSB10では、ACチェック部222は、ACM213に対してステップSB9におけるチェック結果=OKとともに、図8（c）に示した許諾情報242を返却する。これにより、ステップSB11では、ACM213は、MO装置220の復号部223に許諾情報242（図8（c）参照）を転送

する。そして、上記許諾情報242を受信すると、ステップSB12では、復号部223は、MO装置220より鍵Key (=def=K2 (図8(c) 参照)) を取得した後、ステップSB13へ進む。

【0083】ステップSB13では、復号部223は、鍵Key (=def=K2 (図8(c) 参照)) を用いて許諾情報242を図8(d) に示したように復号した後、ステップSB14へ進む。ここでは、図8(d) に示したようにDSN (=456) が復号される。ステップSB14では、復号部223は、復号された許諾情報242 (図8(d) 参照) をACチェック部222へ転送する。

【0084】これにより、ステップSB15では、ACチェック部222は、MO装置220からDSN (=456) を取得した後、ステップSB16へ進む。ステップSB16では、ACチェック部222は、復号された許諾情報242の条件 (DSN=456) と上記DSN (=456) とが一致するか否かを判断する。この場合、両者が一致するため、ACチェック部222は、ステップSB16の判断結果を「Yes」として、ステップSB17へ進む。

【0085】一方、ステップSB16の判断結果が「No」である場合、言い換えれば、両者が一致しない場合、ACチェック部222は、ステップSB26へ進む。ステップSB26では、ACチェック部222は、ACM213にチェック結果=NGを返答する。これにより、ステップSB27では、ACM213は、MPEG2再生部214にチェック結果=NGを返答した後、一連の処理を終了する。つまり、この場合には、許諾情報242に基づく許諾条件 (MSN=123&DSN=456) が満たされていないため、MO媒体240に記録されたコンテンツ241の再生が許諾されない。

【0086】この場合、ステップSB17では、ACチェック部222は、ACM213に対して、ステップSB16におけるチェック結果=OKとともに図8(e) に示した許諾情報242を返却する。これにより、ステップSB18では、ACM213は、MPEG2デコーダ230の復号部232に許諾情報242 (図8(e) 参照) を転送する。そして、上記許諾情報242を受信すると、ステップSB19では、復号部232は、MPEG2デコーダ230より鍵Key (=ghi=K3 (図8(e) 参照)) を取得した後、ステップSB20へ進む。

【0087】ステップSB20では、復号部232は、鍵Key (=ghi=K3 (図8(e) 参照)) を用いて許諾情報242を図8(f) に示したように復号した後、ステップSB21へ進む。ここでは、図8(f) に示したようにDSN (=789) が復号される。ステップSB21では、復号部232は、復号された許諾情報242 (図8(f) 参照) をACチェック部231へ転

送する。

【0088】これにより、ステップSB22では、ACチェック部231は、MPEG2デコーダ230からDSN (=789) を取得した後、ステップSB23へ進む。ステップSB23では、ACチェック部231は、復号された許諾情報242の条件 (DSN=789) と上記DSN (=789) とが一致するか否かを判断する。この場合、両者が一致するため、ACチェック部231は、ステップSB23の判断結果を「Yes」として、ステップSB24へ進む。

【0089】一方、ステップSB23の判断結果が「No」である場合、言い換えれば、両者が一致しない場合、ACチェック部231は、ステップSB26へ進む。ステップSB26では、ACチェック部231は、ACM213にチェック結果=NGを返答する。これにより、ステップSB27では、ACM213は、MPEG2再生部214にチェック結果=NGを返答した後、一連の処理を終了する。つまり、この場合には、許諾情報242に基づく許諾条件 (MSN=123&DSN=456&DSN=789) が満たされていないため、MO媒体240に記録されたコンテンツ241の再生が許諾されない。

【0090】この場合、ステップSB24では、ACチェック部231は、ステップSB23のチェック結果=OKをACM213に返答する。これにより、ステップSB25では、ACM213は、MPEG2再生部214に対して、ステップSB9、ステップSB16およびステップSB23のすべてのチェック結果=OKを返答した後、一連の処理を終了する。つまり、この場合には、MO媒体240に記録された許諾情報242の条件がすべて満たされているため、MO媒体240に記録されたコンテンツ241の再生が許諾される。

【0091】したがって、MPEG2再生部214は、ドライブ221およびファイルシステム212を経由してMO媒体240からコンテンツ241を読み出した後、これをMPEG2デコーダ230へ転送する。これにより、MPEG2デコーダ230においては、コンテンツ241が動画再生される。

【0092】以上説明したように、実施の形態2によれば、図7に示したように複数の部分許諾情報 (MSN123、DSN=456等) を多重暗号化してMO媒体240に記録するようにしたので、コンテンツ241の不正利用を防止することができる。

【0093】(実施の形態3) さて、前述した実施の形態2においては、図5に示したコンテンツ241を暗号化しない例について説明したが、このコンテンツ241を暗号化するようにしてもよい。この場合には、暗号化されたコンテンツ241を復号するためのコンテンツ復号鍵および許諾情報242を多重暗号化してもよい。以下においては、この場合を実施の形態3として説明す

る。

【0094】図10は、本発明にかかる実施の形態3の構成を示すブロック図である。この図において、図5の各部に対応する部分には同一の符号を付ける。図10においては、図5に示したMPEG2デコーダ230に代えてMPEG2デコーダ310が設けられている。さらに図10に示したMO媒体240には、図5に示した許諾情報242に代えて許諾情報300が格納されている。ここで、図10に示したコンテンツ241は、暗号化されている。この暗号化されたコンテンツ241と許諾情報300とは、前述した図6の場合と同様にして関連付けられた状態でMO媒体240に格納されている。

【0095】MPEG2デコーダ310は、ACチェック部311により設定されるコンテンツ復号鍵 K_c を用いて、暗号化されたコンテンツ241（動画データ）を復号し、この復号された結果をデコードすることにより、コンテンツ241を再生する。このMPEG2デコーダ310には、自身の識別情報であるDSN=789が付与されている。復号部312は、MPEG2デコーダ310に格納されている鍵 $Key = ghi$ を用いて、許諾情報300からMSN=789を復号する。ACチェック部311は、許諾情報300の条件（この場合、DSN=789）を満たすか否かをチェックする。

【0096】図11は、実施の形態3におけるライセンス（許諾情報300）の一例を示す図である。この図において、MPEG2デコーダAC: DSN=789およびコンテンツ復号鍵 K_c は、前述した対象物理要素としてのMPEG2デコーダにそれぞれ対応するものであり、鍵 $Key = ghi$ により暗号化されている。このコンテンツ復号鍵 K_c は、暗号化されたコンテンツ241（図10参照）をMPEG2デコーダ310において復号するときに用いられる。また、DSN=789およびコンテンツ復号鍵 K_c は、MPEG2デコーダ310（図10参照）にのつての許諾情報である。

【0097】MO装置AC: DSN=456は、対象物理要素としてのMO装置に対応するものである。このDSN=456と暗号化されたDSN=789およびコンテンツ復号鍵 K_c とは、鍵 $Key = def$ により多重暗号化されている。この多重暗号化されたDSN=456、DSN=789およびコンテンツ復号鍵 K_c は、MO装置220（図10参照）にのつての許諾情報である。

【0098】また、MO媒体AC: MSN=123は、対象物理要素としてのMO媒体に対応するものである。このMSN=123と、多重暗号化されたDSN=456、DSN=789およびコンテンツ復号鍵 K_c とは、鍵 $Key = abc$ により多重暗号化されている。この多重暗号化されたMSN=123、DSN=456、DSN=789およびコンテンツ復号鍵 K_c は、MO媒体240（図1参照）にのつての許諾情報である。

【0099】つぎに、上述した実施の形態3の動作について図13に示したフローチャートを参照しつつ説明する。この場合、図10に示したMO装置220のドライブ221には、MO媒体240がセットされているものとする。この状態において、図13に示したステップSC1でユーザUからMPEG2再生部214に対してMPEG2（コンテンツ）の再生が指示されると、ステップSC2では、MPEG2再生部214は、ACM213に対してMPEG2（コンテンツ）の再生を指示する。

【0100】これにより、ステップSC3では、ACM213は、MO媒体240から、ファイルシステム212経由で暗号化された図12（a）に示した許諾情報300を取得した後、ステップSC4へ進む。ステップSC4では、ACM213は、取得した許諾情報300（図12（a）参照）をMO装置220の復号部223へ転送する。これにより、ステップSC5では、復号部223は、MO媒体240から鍵 $Key (= abc = K1)$ （図12（a）参照）を取得した後、ステップSC6へ進む。

【0101】ステップSC6では、復号部223は、鍵 $Key (= abc = K1)$ （図12（a）参照）を用いて許諾情報300を図12（b）に示したように復号した後、ステップSC7へ進む。ここでは、図12（b）に示したようにMSN（=123）が復号される。ステップSC7では、復号部223は、復号された許諾情報300をACチェック部222へ転送する。

【0102】これにより、ステップSC8では、ACチェック部222は、MO媒体240からMSN（=123）を取得した後、ステップSC9へ進む。ステップSC9では、ACチェック部222は、復号された図12（b）に示した許諾情報300の条件（MSN=123）と上記MSN（=123）とが一致するか否かを判断する。この場合、両者が一致するため、ACチェック部222は、ステップSC9の判断結果を「Yes」として、ステップSC10へ進む。

【0103】一方、ステップSC9の判断結果が「No」である場合、すなわち、両者が一致しない場合、ACチェック部222は、ステップSC27へ進む。ステップSC27では、ACチェック部222は、ACM213にチェック結果=NGを返答する。これにより、ステップSC28では、ACM213は、MPEG2再生部214にチェック結果=NGを返答した後、一連の処理を終了する。つまり、この場合には、許諾情報300に基づく許諾条件（MSN=123）が満たされていないため、MO媒体240に記録されたコンテンツ241の再生が許諾されない。

【0104】この場合、ステップSC10では、ACチェック部222は、ACM213に対してステップSC9におけるチェック結果=OKとともに、図12（c）

に示した許諾情報300を返却する。これにより、ステップSC11では、ACM213は、MO装置220の復号部223に許諾情報300（図12（c）参照）を転送する。そして、上記許諾情報300を受信すると、ステップSC12では、復号部223は、MO装置220より鍵Key（=def=K2（図12（c）参照））を取得した後、ステップSC13へ進む。

【0105】ステップSC13では、復号部223は、鍵Key（=def=K2（図12（c）参照））を用いて許諾情報300を図12（d）に示したように復号した後、ステップSC14へ進む。ここでは、図12（d）に示したようにDSN（=456）が復号される。ステップSC14では、復号部223は、復号された許諾情報300（図12（d）参照）をACチェック部222へ転送する。

【0106】これにより、ステップSC15では、ACチェック部222は、MO装置220からDSN（=456）を取得した後、ステップSC16へ進む。ステップSC16では、ACチェック部222は、復号された許諾情報300の条件（DSN=456）と上記DSN（=456）とが一致するか否かを判断する。この場合、両者が一致するため、ACチェック部222は、ステップSC16の判断結果を「Yes」として、ステップSC17へ進む。

【0107】一方、ステップSC16の判断結果が「No」である場合、言い換えれば、両者が一致しない場合、ACチェック部222は、ステップSC27へ進む。ステップSC27では、ACチェック部222は、ACM213にチェック結果=NGを返答する。これにより、ステップSC28では、ACM213は、MPEG2再生部214にチェック結果=NGを返答した後、一連の処理を終了する。つまり、この場合には、許諾情報300に基づく許諾条件（MSN=123&DSN=456）が満たされていないため、MO媒体240に記録されたコンテンツ241の再生が許諾されない。

【0108】この場合、ステップSC17では、ACチェック部222は、ACM213に対して、ステップSC16におけるチェック結果=OKとともに図12

（e）に示した許諾情報300を返却する。これにより、ステップSC18では、ACM213は、MPEG2デコーダ310の復号部312に許諾情報300（図12（e）参照）を転送する。そして、上記許諾情報300を受信すると、ステップSC19では、復号部312は、MPEG2デコーダ310より鍵Key（=ghi=K3（図12（e）参照））を取得した後、ステップSC20へ進む。

【0109】ステップSC20では、復号部312は、鍵Key（=ghi=K3（図12（e）参照））を用いて許諾情報300を図12（f）に示したように復号した後、ステップSC21へ進む。ここでは、図12

（f）に示したようにDSN（=789）が復号される。ステップSC21では、復号部312は、復号された許諾情報300（図12（f）参照）をACチェック部311へ転送する。

【0110】これにより、ステップSC22では、ACチェック部311は、MPEG2デコーダ310からDSN（=789）を取得した後、ステップSC23へ進む。ステップSC23では、ACチェック部311は、復号された許諾情報300の条件（DSN=789）と上記DSN（=789）とが一致するか否かを判断する。この場合、両者が一致するため、ACチェック部311は、ステップSC23の判断結果を「Yes」として、ステップSC24へ進む。

【0111】一方、ステップSC23の判断結果が「No」である場合、言い換えれば、両者が一致しない場合、ACチェック部311は、ステップSC27へ進む。ステップSC27では、ACチェック部311は、ACM213にチェック結果=NGを返答する。これにより、ステップSC28では、ACM213は、MPEG2再生部214にチェック結果=NGを返答した後、一連の処理を終了する。つまり、この場合には、許諾情報300に基づく許諾条件（MSN=123&DSN=456&DSN=789）が満たされていないため、MO媒体240に記録されたコンテンツ241の再生が許諾されない。

【0112】この場合、ステップSC24では、ACチェック部311は、MPEG2デコーダ310にコンテンツ復号鍵Kcを設定した後、ステップSC25へ進む。ステップSC25では、ACチェック部311は、ステップSC23のチェック結果=OKをACM213に返答する。これにより、ステップSC26では、ACM213は、MPEG2再生部214に対して、ステップSC9、ステップSC16およびステップSC23のすべてのチェック結果=OKを返答した後、一連の処理を終了する。つまり、この場合には、MO媒体240に記録された許諾情報300の条件がすべて満たされているため、MO媒体240に記録されたコンテンツ241の再生が許諾される。

【0113】したがって、MPEG2再生部214は、ドライブ221およびファイルシステム212を経由してMO媒体240から暗号化されたコンテンツ241を読み出した後、これをMPEG2デコーダ310へ転送する。これにより、MPEG2デコーダ310においては、ステップSC24で設定されたコンテンツ復号鍵Kcを用いて復号されたコンテンツ241が動画再生される。

【0114】以上説明したように、実施の形態3によれば、図11に示したように複数の部分許諾情報（MSN=123、DSN=456等）に加えてコンテンツ241を復号するためのコンテンツ復号鍵Kcを多重暗号

化してMO媒体240に記録するようにしたので、コンテンツ241の不正利用をより効果的に防止することができる。

【0115】(実施の形態4) 前述した実施の形態3においては、図10に示したファイルシステム212がMO媒体240から許諾情報を無条件で読み出す例について説明したが、セキュリティをさらに高める目的で、MO媒体240上のセキュア領域(暗号化領域)に暗号化された許諾情報を格納し、この暗号化された許諾情報を復号することができるファイルシステムのみが許諾情報を読み出すことができるようにしてもよい。以下においては、この場合を実施の形態4として説明する。

【0116】図14は、本発明にかかる実施の形態4の構成を示すブロック図である。この図において、図10の各部に対応する部分には同一の符号を付ける。図14においては、図10に示したMO媒体240および計算機210に代えて、MO媒体440および計算機400が設けられている。

【0117】図14に示したMO媒体440は、図15に示したように、暗号化されたコンテンツ441が格納される非セキュア領域A₁と、暗号化された許諾情報442が格納されるセキュア領域A₂とを有している。ここで、非セキュア領域A₁は、ユーザ領域であり、一般のファイルシステムであればアクセス可能な領域である。一方、セキュア領域A₂は、一般のファイルシステムがアクセスできない領域であり、図14に示した復号器411を有するファイルシステム410のみがアクセス可能な領域である。

【0118】図15に示した許諾情報442は、前述した許諾情報300(図10および図11参照)が暗号化されたものである。したがって、許諾情報442には、図11に示したMSN=123、DSN=456、DSN=789およびコンテンツ復号鍵K_cが含まれている。また、図15において、許諾情報442は、補助ファイル管理データD_{C2}により管理される。

【0119】一方、非セキュア領域A₁において、ファイル管理データD_{C1}は、コンテンツ441を管理するためのデータであるとともに、補助ファイル管理データD_{C2}を介して許諾情報442を間接的に管理するためのデータである。このように、MO媒体440においては、コンテンツ441と許諾情報442がファイル管理データD_{C1}および補助ファイル管理データD_{C2}を介して関連付けられている。図14に戻り、計算機400のファイルシステム410は、MO媒体440から許諾情報442、コンテンツ441、鍵Key=a b c、MSN=123をそれぞれ読み出す。復号器411は、暗号化された許諾情報442を復号する。

【0120】つぎに、上述した実施の形態4の動作について図16および図17に示したフローチャートを参照しつつ説明する。この場合、図14に示したMO装置2

20のドライブ221には、MO媒体440がセットされているものとする。この状態において、図16に示したステップSD1でユーザUからMPEG2再生部214に対してMPEG2(コンテンツ)の再生が指示されると、ステップSD2では、MPEG2再生部214は、ACM213に対してMPEG2(コンテンツ)の再生を指示する。

【0121】これにより、ステップSD3では、ファイルシステム410は、MO媒体440のセキュア領域A₂(図15参照)にアクセスし、暗号化された許諾情報442を取得した後、これを復号器411へ渡す。ステップSD4では、復号器411は、暗号化された許諾情報442(図15参照)を所定の鍵を用いて復号した後、ステップSD5へ進む。ステップSD5では、復号器411は、復号された許諾情報442をACM213に転送する。

【0122】これにより、図17に示したステップSD6では、ACM213は、復号された許諾情報442をMO装置220の復号部223に転送する。ステップSD7では、復号部223は、MO媒体440から鍵Key(=a b c=K1(図12(a)参照))を取得した後、ステップSD8へ進む。ステップSD8では、復号部223は、鍵Key(=a b c)を用いて許諾情報442を図12(b)に示したように復号した後、ステップSD9へ進む。ここでは、図12(b)に示したようにMSN(=123)が復号される。ステップSD9では、復号部223は、復号された許諾情報442をACチェック部222へ転送する。

【0123】これにより、ステップSD10では、ACチェック部222は、MO媒体440からMSN(=123)を取得した後、ステップSD11へ進む。ステップSD11では、ACチェック部222は、復号された図12(b)に示した許諾情報442の条件(MSN=123)と上記MSN(=123)とが一致するか否かを判断する。この場合、両者が一致するため、ACチェック部222は、ステップSD11の判断結果を「Yes」として、ステップSD12へ進む。

【0124】一方、ステップSD11の判断結果が「No」である場合、すなわち、両者が一致しない場合、ACチェック部222は、ステップSD29へ進む。ステップSD29では、ACチェック部222は、ACM213にチェック結果=NGを返答する。これにより、ステップSD30では、ACM213は、MPEG2再生部214にチェック結果=NGを返答した後、一連の処理を終了する。つまり、この場合には、許諾情報442に基づく許諾条件(MSN=123)が満たされていないため、MO媒体440に記録されたコンテンツ441の再生が許諾されない。

【0125】この場合、ステップSD12では、ACチェック部222は、ACM213に対してステップSD

11におけるチェック結果＝OKとともに、許諾情報442（図12（c）参照）を返却する。これにより、ステップSD13では、ACM213は、MO装置220の復号部223に許諾情報442（図12（c）参照）を転送する。そして、上記許諾情報442を受信すると、ステップSD14では、復号部223は、MO装置220より鍵Key（＝def＝K2（図12（c）参照））を取得した後、ステップSD15へ進む。

【0126】ステップSD15では、復号部223は、鍵Key（＝def＝K2（図12（c）参照））を用いて許諾情報442を図12（d）に示したように復号した後、ステップSD16へ進む。ここでは、図12（d）に示したようにDSN（＝456）が復号される。ステップSD16では、復号部223は、復号された許諾情報442（図12（d）参照）をACチェック部222へ転送する。

【0127】これにより、ステップSD17では、ACチェック部222は、MO装置220からDSN（＝456）を取得した後、ステップSD18へ進む。ステップSD18では、ACチェック部222は、復号された許諾情報442の条件（DSN＝456）と上記DSN（＝456）とが一致するか否かを判断する。この場合、両者が一致するため、ACチェック部222は、ステップSD18の判断結果を「Yes」として、ステップSD19へ進む。

【0128】一方、ステップSD18の判断結果が「No」である場合、言い換えれば、両者が一致しない場合、ACチェック部222は、ステップSD29へ進む。ステップSD29では、ACチェック部222は、ACM213にチェック結果＝NGを返答する。これにより、ステップSD30では、ACM213は、MPEG2再生部214にチェック結果＝NGを返答した後、一連の処理を終了する。つまり、この場合には、許諾情報442に基づく許諾条件（MSN＝123&DSN＝456）が満たされていないため、MO媒体440に記録されたコンテンツ441の再生が許諾されない。

【0129】この場合、ステップSD19では、ACチェック部222は、ACM213に対して、ステップSD18におけるチェック結果＝OKとともに図12

（e）に示した許諾情報442を返却する。これにより、ステップSD20では、ACM213は、MPEG2デコーダ310の復号部312に許諾情報442（図12（e）参照）を転送する。そして、上記許諾情報442を受信すると、ステップSD21では、復号部312は、MPEG2デコーダ310より鍵Key（＝ghi＝K3（図12（e）参照））を取得した後、ステップSD22へ進む。

【0130】ステップSD22では、復号部312は、鍵Key（＝ghi＝K3（図12（e）参照））を用いて許諾情報442を図12（f）に示したように復号

した後、ステップSD23へ進む。ここでは、図12（f）に示したようにDSN（＝789）が復号される。ステップSD23では、復号部312は、復号された許諾情報442（図12（f）参照）をACチェック部311へ転送する。

【0131】これにより、ステップSD24では、ACチェック部311は、MPEG2デコーダ310からDSN（＝789）を取得した後、ステップSD25へ進む。ステップSD25では、ACチェック部311は、復号された許諾情報442の条件（DSN＝789）と上記DSN（＝789）とが一致するか否かを判断する。この場合、両者が一致するため、ACチェック部311は、ステップSD25の判断結果を「Yes」として、ステップSD26へ進む。

【0132】一方、ステップSD25の判断結果が「No」である場合、言い換えれば、両者が一致しない場合、ACチェック部311は、ステップSD29へ進む。ステップSD29では、ACチェック部311は、ACM213にチェック結果＝NGを返答する。これにより、ステップSD30では、ACM213は、MPEG2再生部214にチェック結果＝NGを返答した後、一連の処理を終了する。つまり、この場合には、許諾情報442に基づく許諾条件（MSN＝123&DSN＝456&DSN＝789）が満たされていないため、MO媒体440に記録されたコンテンツ441の再生が許諾されない。

【0133】この場合、ステップSD26では、ACチェック部311は、MPEG2デコーダ310にコンテンツ復号鍵K_cを設定した後、ステップSD27へ進む。ステップSD27では、ACチェック部311は、ステップSD26のチェック結果＝OKをACM213に返答する。これにより、ステップSD28では、ACM213は、MPEG2再生部214に対して、ステップSD11、ステップSD18およびステップSD25のすべてのチェック結果＝OKを返答した後、一連の処理を終了する。つまり、この場合には、MO媒体440に記録された許諾情報442の条件がすべて満たされているため、MO媒体440に記録されたコンテンツ441の再生が許諾される。

【0134】したがって、MPEG2再生部214は、ドライブ221およびファイルシステム410を経由してMO媒体440から暗号化されたコンテンツ441を読み出した後、これをMPEG2デコーダ310へ転送する。これにより、MPEG2デコーダ310においては、ステップSD26で設定されたコンテンツ復号鍵K_cを用いて復号されたコンテンツ441が動画再生される。

【0135】つぎに、図14に示した許諾情報442を、コンテンツ441、鍵Key＝abcおよびMSN＝123が既に格納されているMO媒体440に書き込

むデータ書込装置について、図18を参照しつつ説明する。つまり、MO媒体440には、許諾情報442が格納されていない。この図において、計算機460は、駅、コンビニエンスストア等に設置されており、許諾情報を購入する装置である。この計算機460においては、許諾情報を購入するための許諾情報購入アプリケーションプログラム461が起動される。OS462は、許諾情報購入アプリケーションプログラム461を制御する。

【0136】ファイルシステム463は、計算機460で扱われるファイルを管理し、データのリード/ライトを制御する。暗号器464は、MO媒体440に対して書き込むべきデータを暗号化する。ライセンスサーバ450は、コンテンツ提供者側に設置されており、ネットワークNを介して計算機460に接続されている。このライセンスサーバ450は、許諾情報を販売するためのものである。MO装置470は、計算機460に外付け（または内蔵）されており、MO媒体（同図の場合、MO媒体440）に対してデータを書き込む。このMO装置470は、MO媒体を駆動するドライブ471を有している。

【0137】つぎに、図19を参照して図18に示したデータ書込装置の動作について説明する。この図に示したステップSE1では、ユーザUは、図示しない入力装置を用いて、ファイル名（たとえば、曲名）、サーバ名等のパラメータを入力することにより、許諾情報442の購入を指示する。これにより、ステップSE2では、許諾情報購入アプリケーションプログラム461は、ネットワークNを介してライセンスサーバ450から許諾情報442を購入（取得）した後、ステップSE3へ進む。

【0138】ステップSE3では、許諾情報購入アプリケーションプログラム461は、許諾情報442をファイルシステム463へ転送する。これにより、ステップSE4では、ファイルシステム463の暗号器464は、所定の鍵を用いて許諾情報442を暗号化する。つぎのステップSE5では、ファイルシステム463は、MO装置470を経由してMO媒体440のセキュア領域A₂（図15参照）に暗号化された許諾情報442を格納する。

【0139】以上説明したように、実施の形態4によれば、図15に示したように、MO媒体440のセキュア領域A₂に暗号化された許諾情報442を記録するようにしたので、コンテンツ441の不正利用を防止することができる。

【0140】（実施の形態5）図20は、本発明にかかる実施の形態5の構成を示すブロック図である。この図において、図10の各部に対応する部分には同一の符号を付ける。図20においては、図10に示したMO媒体240、計算機210およびMO装置220に代えて、

MO媒体540、計算機500およびMO装置520が設けられている。

【0141】図20に示したMO媒体540は、図21に示したように、通常領域B₁、特別領域B₂および媒体管理用領域B₃を有している。通常領域B₁は、コンテンツ541（図20参照）が格納される領域であり、この通常領域B₁の範囲は、PSN（Physical Sector Number：物理セクタ番号）=M+1～Nまでとされている。特別領域B₂は、後述する相互認証コマンド（特別なコマンド）が発行された場合のみアクセスが可能な領域であり、許諾情報542（図20参照）が格納されている。この許諾情報542は、前述した許諾情報300と同一のデータ構造（図11参照）である。また、この特別領域B₂の範囲は、PSN=L～Mまでとされている。

【0142】媒体管理用領域B₃には、MO媒体540における通常領域B₁および特別領域B₂の範囲を定義する媒体管理テーブルTが格納されている。この媒体管理テーブルTには、通常領域B₁および特別領域B₂の開始PSN（物理セクタ番号における先頭番号）と、通常領域B₁および特別領域B₂の終了PSN（物理セクタ番号における末尾番号）とがそれぞれ定義されている。また、この媒体管理用領域B₃の範囲は、PSN=1～Lまでとされている。

【0143】図20に戻り、MO媒体540には、上述したコンテンツ541、許諾情報542の他に、MO媒体240（図10参照）と同様に、鍵Key=abc、MSN=123がそれぞれ格納されている。計算機500において、ファイルシステム510は、計算機500で扱われるファイルを管理し、データのリード/ライトを制御する。相互認証モジュール511は、MO装置520の相互認証モジュール521が有する秘密情報（以下、MO装置側秘密情報と称する）と共通の秘密情報（以下、計算機側秘密情報と称する）を保持している。

【0144】また、相互認証モジュール511は、上述した相互認証コマンドが発行されたとき、相互認証モジュール521との間で相互認証を行う。具体的には、相互認証モジュール511は、計算機側秘密情報を相互認証モジュール521へ送信し、相互認証モジュール521からのMO装置側秘密情報と自身が保持する計算機側秘密情報とが一致するか否かにより相互認証を行う。ここで、ファイルシステム510は、相互認証された場合にのみMO媒体540の特別領域B₂から許諾情報542を読み出すことが可能である。

【0145】MO装置520において、相互認証モジュール521は、上述したように、ファイルシステム510の相互認証モジュール511が有する計算機側秘密情報と共通のMO装置側秘密情報を保持している。相互認証モジュール521は、相互認証モジュール511から

の計算機側秘密情報を受信したとき、自身が保持するMO装置側秘密情報を相互認証モジュール511へ送信する。また、相互認証モジュール521は、相互認証モジュール511からの計算機側秘密情報と自身が保持するMO装置側秘密情報とが一致するか否かにより相互認証を行う。

【0146】つぎに、実施の形態5の動作について、図22および図13に示したフローチャートを参照しつつ説明する。この場合、図20に示したMO装置520のドライブ221には、MO媒体540がセットされているものとする。この状態において、図22に示したステップSF1でユーザUからMPEG2再生部214に対してMPEG2（コンテンツ）の再生が指示されると、ステップSF2では、MPEG2再生部214は、ACM213に対してMPEG2（コンテンツ）の再生を指示する。

【0147】これにより、ステップSF3では、ACM213からファイルシステム510に対して相互認証コマンドが発行され、相互認証モジュール511と相互認証モジュール521との間で相互認証が行われる。すなわち、ファイルシステム510の相互認証モジュール511は、MO装置520の相互認証モジュール521へ計算機側秘密情報を送信する。そして、この計算機側秘密情報を受信すると、相互認証モジュール521は、相互認証モジュール511へMO装置側秘密情報を送信する。

【0148】つぎに、相互認証モジュール521は、受信した計算機側秘密情報と自身が保有するMO装置側秘密情報とが一致するか否かを判断し、この判断結果を相互認証モジュール511へ渡す。一方、相互認証モジュール511は、相互認証モジュール521からのMO装置側秘密情報を受信すると、受信したMO装置側秘密情報と自身が保持する計算機側秘密情報とが一致するか否かを判断する。

【0149】そして、ステップSF4では、ファイルシステム510は、相互認証モジュール511側の相互認証に関する判断結果と、相互認証モジュール521側の相互認証に関する判断結果との双方に基づいて、相互認証がとられたか否かを判断する。ここで、双方の判断結果が共に「一致」である場合、ファイルシステム510は、相互認証結果=OKをACM213へ渡し、ステップSF4の判断結果を「Yes」とする。

【0150】これにより、図13に示したステップSC3では、ACM213は、ファイルシステム510経由でMO媒体540の特別領域B₂から許諾情報542を取得する。以後、前述した実施の形態3と同様にして、ステップSC4～ステップSC28までの処理が実行される。なお、実施の形態5においては、図13に示したMO媒体240、許諾情報300、コンテンツ241、ファイルシステム212およびMO装置220を、MO

媒体540、許諾情報542、コンテンツ541、ファイルシステム510およびMO装置520と読み替えるものとする。

【0151】一方、図22に示したステップSF4において、相互認証モジュール511側の相互認証に関する判断結果と、相互認証モジュール521側の相互認証に関する判断結果との双方が共に「不一致」である場合、判断結果を「No」として、図13に示したステップSC27へ進む。ステップSC17では、ファイルシステム510は、相互認証結果=NGをACM213へ渡す。この場合には、相互認証がとられなかったため、図20に示したMO媒体540の特別領域B₂からは、許諾情報542が読み出されることがない。

【0152】つぎに、図20に示したMO媒体540に通常領域B₁および特別領域B₂を設定するフォーマット装置について、図23を参照して説明する。この図に示した計算機560は、MO媒体540に対して物理フォーマットを行う装置である。フォーマッタ561は、MO媒体540の物理フォーマットに関する制御を行う。OS562は、各種アプリケーションプログラムを制御する。デバイスドライバ563は、MO装置570を駆動するものである。MO装置570は、計算機560に外付け（または内蔵）されている。このMO装置570は、MO媒体を駆動するドライブ571および物理フォーマットを行う。

【0153】つぎに、図24を参照して図23に示したフォーマット装置の動作について説明する。この図に示したステップSG1では、ユーザUは、図示しない入力装置を用いて、セキュア領域（特別領域B₂（図21参照））のサイズを指定することにより、MO媒体540のフォーマットを指示する。これにより、ステップSG2では、フォーマッタ561は、デバイスドライバ563経由で物理フォーマット部572に対して物理フォーマットを指示する。これにより、ステップSG3では、物理フォーマット部572は、MO媒体540に対する物理フォーマットを実行する。これにより、MO媒体540には、通常領域B₁および特別領域B₂が形成される。

【0154】以上説明したように、実施の形態5によれば、図21に示したMO媒体540の特別領域B₂に許諾情報542を記録し、二つの相互認証モジュール511、相互認証モジュール521で相互認証がとられた場合にのみ、該特別領域B₂から許諾情報542を取得するようにしたので、相互認証がとられない場合に、即時に許諾不可とすることができ、コンテンツ541の不正利用を防止することができる。

【0155】（実施の形態6）さて、前述した実施の形態4においては、図15に示したようにMO媒体440に非セキュア領域A₁およびセキュア領域A₂を確保した例について説明した。また、実施の形態5において

は、図21に示したようにMO媒体540に通常領域B₁および特別領域B₂を確保した例について説明した。以下においては、実施の形態4（非セキュア領域A₁、セキュア領域A₂）と実施の形態5（通常領域B₁、特別領域B₂）とを組み合わせた例を実施の形態6として説明する。

【0156】実施の形態6においては、図25に示したMO媒体600が用いられる。すなわち、同図に示したMO媒体600においては、通常領域B₁（図21参照）と非セキュア領域A₁（図15参照）とがマッピングされているとともに、特別領域B₂（図21参照）とセキュア領域A₂（図15参照）とがマッピングされている。また、通常領域B₁（非セキュア領域A₁）には、コンテンツ441およびこれを管理するためのファイル管理データD_{C1}が格納されている。一方、特別領域B₂（セキュア領域A₂）には、許諾情報442およびこれを管理するための補助ファイル管理データD_{C2}が格納されている。

【0157】以上説明したように、実施の形態6によれば、いずれもセキュリティ上有効である特別領域B₂にセキュア領域A₂をマッピングするようにしたので、極めて高いセキュリティを確保することができる。

【0158】（実施の形態7）さて、前述した実施の形態1～6においては、MO媒体に格納されたコンテンツおよび許諾情報（AC）を別のMO媒体に転送するようにしてもよい。以下、この場合を実施の形態7として説明する。図26は、本発明にかかる実施の形態7におけるバックドデータ生成装置の構成を示すブロック図であり、図27は、同実施の形態7におけるアンパック装置の構成を示すブロック図である。

【0159】これらのバックドデータ生成装置（図26参照）とアンパック装置（図27参照）とは図示しないケーブル、ネットワーク等を介して接続されている。図26に示したバックドデータ生成装置は、MO媒体800に格納された許諾情報801および暗号化コンテンツ802をひとまとまりのデータ（バックドデータ830）として、これをアンパック装置（図27参照）へ転送する装置である。

【0160】図26において、MO媒体800に格納された許諾情報801は、前述した実施の形態1～6のうちいずれかの許諾情報（AC）である。この許諾情報801には、MSNおよび鍵Keyが含まれている。暗号化コンテンツ802は、暗号化されたコンテンツである。計算機820は、送信側に設置されている。OS821は、各種アプリケーションプログラムの実行を制御する。ファイルシステム822は、計算機820で扱われるファイルを管理し、データのリード/ライトを制御する。

【0161】バック処理部823は、許諾情報801と暗号化コンテンツ802とから一つのファイル（バック

ドデータ830）を生成する。転送部824は、バックドデータ830をアンパック装置（図27参照）転送する。MO装置810は、計算機820に外付け（または内蔵）されており、MO媒体（同図の場合、MO媒体800）から許諾情報801および暗号化コンテンツ802を読み出す。このMO装置810は、MO媒体を駆動するドライブ811を有している。

【0162】一方、図27において、計算機920は、受信側に設置されている。OS921は、各種アプリケーションプログラムの実行を制御する。ファイルシステム922は、計算機920で扱われるファイルを管理し、データのリード/ライトを制御する。受信部924は、バックドデータ生成装置（図26参照）から転送されたバックドデータ830を受信する。アンパック処理部923は、上記バックドデータ830から二つのファイル（許諾情報801、暗号化コンテンツ802）を生成する。MO装置910は、計算機920に外付け（または内蔵）されており、MO媒体（同図の場合、MO媒体900）に許諾情報801および暗号化コンテンツ802を書き込む。このMO装置910は、MO媒体を駆動するドライブ911を有している。

【0163】上記構成において、図26に示したMO媒体800から許諾情報801および暗号化コンテンツ802が読み出されると、バック処理部823は、これら許諾情報801と暗号化コンテンツ802とから一つのファイル（バックドデータ830）を生成し、これを転送部824へ渡す。これにより、転送部824は、ケーブル、ネットワーク等を介して図27に示したアンパック装置へバックドデータ830転送する。

【0164】そして、バックドデータ830が図27に示した受信部924に受信されると、アンパック処理部923は、バックドデータ830から許諾情報801および暗号化コンテンツ802を生成する。これにより、MO媒体900には、許諾情報801および暗号化コンテンツ802が書き込まれる。このようにして、実施の形態7においては、MO媒体800からMO媒体900へ許諾情報801および暗号化コンテンツ802を転送（コピー）できるようにしたので、コンテンツの再生に関する許諾（ライセンス）を容易に譲渡することができる。

【0165】以上説明したように、実施の形態7によれば、一方のメディア800から他方のメディア900へ暗号化コンテンツ802および許諾情報801が転送（コピー）されるので、コンテンツ801の利用に関する許諾（ライセンス）を第三者に譲渡することができる。

【0166】以上本発明にかかる実施の形態1～7について図面を参照して詳述してきたが、具体的な構成例はこれら実施の形態1～7に限られるものではなく、本発明の要旨を逸脱しない範囲の設計変更等があっても本発

明に含まれる。

【0167】たとえば、前述した実施の形態1～7においては、コンテンツ利用制御装置、利用制御システムの機能を実現するためのコンテンツ利用制御プログラムをコンピュータ読み取り可能な記録媒体に記録して、この記録媒体に記録されたコンテンツ利用制御プログラムをコンピュータに読み込ませ、実行することによりコンテンツ利用制御を行うようにしてもよい。なお、記録媒体には、光ディスク、フロッピーディスク、ハードディスク等の可搬型の記録媒体が含まれることはもとより、ネットワークのようにデータを一時的に記録保持するような伝送媒体も含まれる。

【0168】

【発明の効果】以上説明したように、請求項1、8にかかる発明によれば、許諾情報とコンテンツとを関連付けて一つのメディアに記録し、この許諾情報および識別情報に基づいて、コンテンツの利用の制御を行うようにしたので、一つのメディアを入手することで同時に許諾情報とコンテンツとが得られるため、許諾情報とコンテンツと別々に入手していた従来に比して、コンテンツを容易に利用することができるという効果を奏する。

【0169】また、請求項2にかかる発明によれば、複数の部分許諾情報を多重暗号化してメディアに記録するようにしたので、コンテンツの不正利用を防止することができるという効果を奏する。

【0170】また、請求項3にかかる発明によれば、複数の部分許諾情報に加えてコンテンツを復号するためのコンテンツ復号鍵を多重暗号化してメディアに記録するようにしたので、コンテンツの不正利用をより効果的に防止することができるという効果を奏する。

【0171】また、請求項4にかかる発明によれば、メディアのセキュア領域に暗号化された許諾情報を記録するようにしたので、コンテンツの不正利用を防止することができるという効果を奏する。

【0172】また、請求項5にかかる発明によれば、メディアの特別領域に許諾情報を記録し、二つの物理要素間で相互認証がとられた場合にのみ、該特別領域から許諾情報を取得するようにしたので、相互認証がとられない場合に、即時に許諾不可とすることができ、コンテンツの不正利用を防止することができるという効果を奏する。

【0173】また、請求項6にかかる発明によれば、いずれもセキュリティ上有効である特別領域にセキュア領域をマッピングするようにしたので、極めて高いセキュリティを確保することができるという効果を奏する。

【0174】また、請求項7にかかる発明によれば、一方のメディアから他方のメディアへコンテンツおよび許諾情報が転送（コピー）されるので、コンテンツの利用に関する許諾（ライセンス）を第三者に譲渡することができるという効果を奏する。

【図面の簡単な説明】

【図1】本発明にかかる実施の形態1の構成を示すブロック図である。

【図2】図1に示したコンテンツ141とAC142との関係を示す図である。

【図3】図1に示したAC142のフォーマットの一例を示す図である。

【図4】同実施の形態1の動作を説明するフローチャートである。

【図5】本発明にかかる実施の形態2の構成を示すブロック図である。

【図6】図5に示したコンテンツ241と許諾情報242との関係を示す図である。

【図7】図5に示したAC242のフォーマットの一例を示す図である。

【図8】図5に示した許諾情報242の一例を示す図である。

【図9】同実施の形態2の動作を説明するフローチャートである。

【図10】本発明にかかる実施の形態3の構成を示すブロック図である。

【図11】同実施の形態3におけるライセンスの一例を示す図である。

【図12】図10に示した許諾情報300の一例を示す図である。

【図13】同実施の形態3の動作を説明するフローチャートである。

【図14】本発明にかかる実施の形態4の構成を示すブロック図である。

【図15】図14に示したMO媒体440におけるデータ構造を示す図である。

【図16】同実施の形態4の動作を説明するフローチャートである。

【図17】同実施の形態4の動作を説明するフローチャートである。

【図18】同実施の形態4におけるデータ書込装置の構成を示すブロック図である。

【図19】図18に示したデータ書込装置の動作を説明するフローチャートである。

【図20】本発明にかかる実施の形態5の構成を示すブロック図である。

【図21】図20に示したMO媒体540におけるデータ構造を示す図である。

【図22】同実施の形態5の動作を説明するフローチャートである。

【図23】同実施の形態5におけるフォーマット装置の構成を示すブロック図である。

【図24】図23に示したフォーマット装置の動作を説明するフローチャートである。

【図25】本発明にかかる実施の形態6におけるMO媒

体600のデータ構造を説明する図である。

【図26】本発明にかかる実施の形態7におけるバックドデータ生成装置の構成を示すブロック図である。

【図27】同実施の形態7におけるアンバック装置の構成を示すブロック図である。

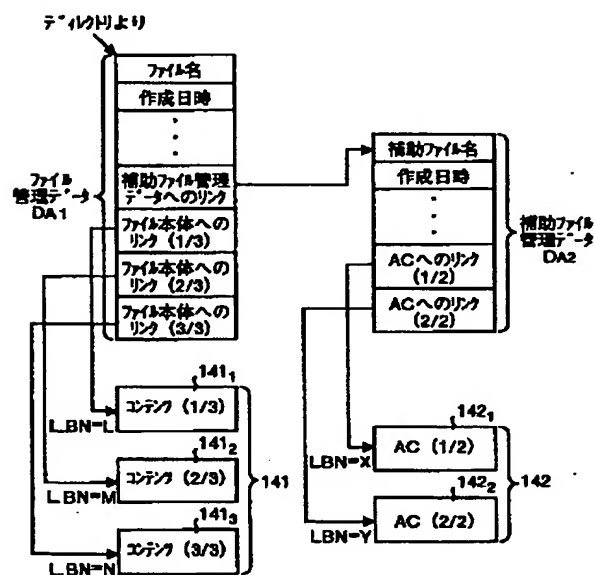
【符号の説明】

110 計算機
112 ファイルシステム
114 MPEG2再生部
120 MO装置
130 MPEG2デコーダ
140 MO媒体
210 計算機
220 MO装置
240 MO媒体

400 計算機
440 MO媒体
400 計算機
500 計算機
511 相互認証モジュール
520 MO装置
521 相互認証モジュール
540 MO媒体
560 計算機
570 MO装置
800 MO媒体
820 計算機
824 転送部
920 計算機
924 受信部

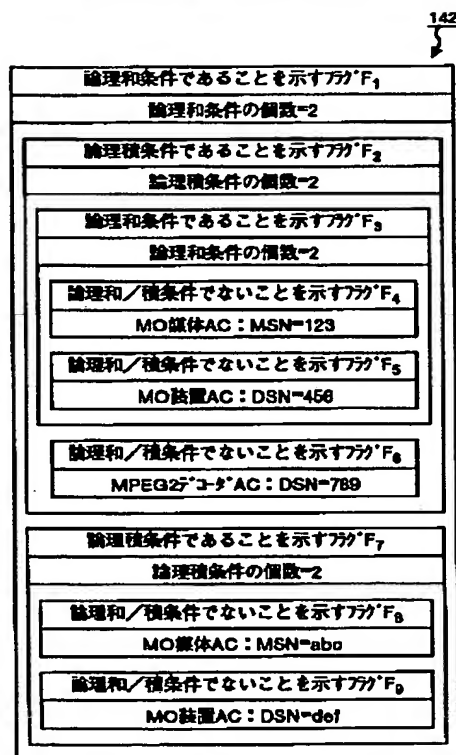
【図2】

図1に示したエンタ141とAC142との関係を示す図

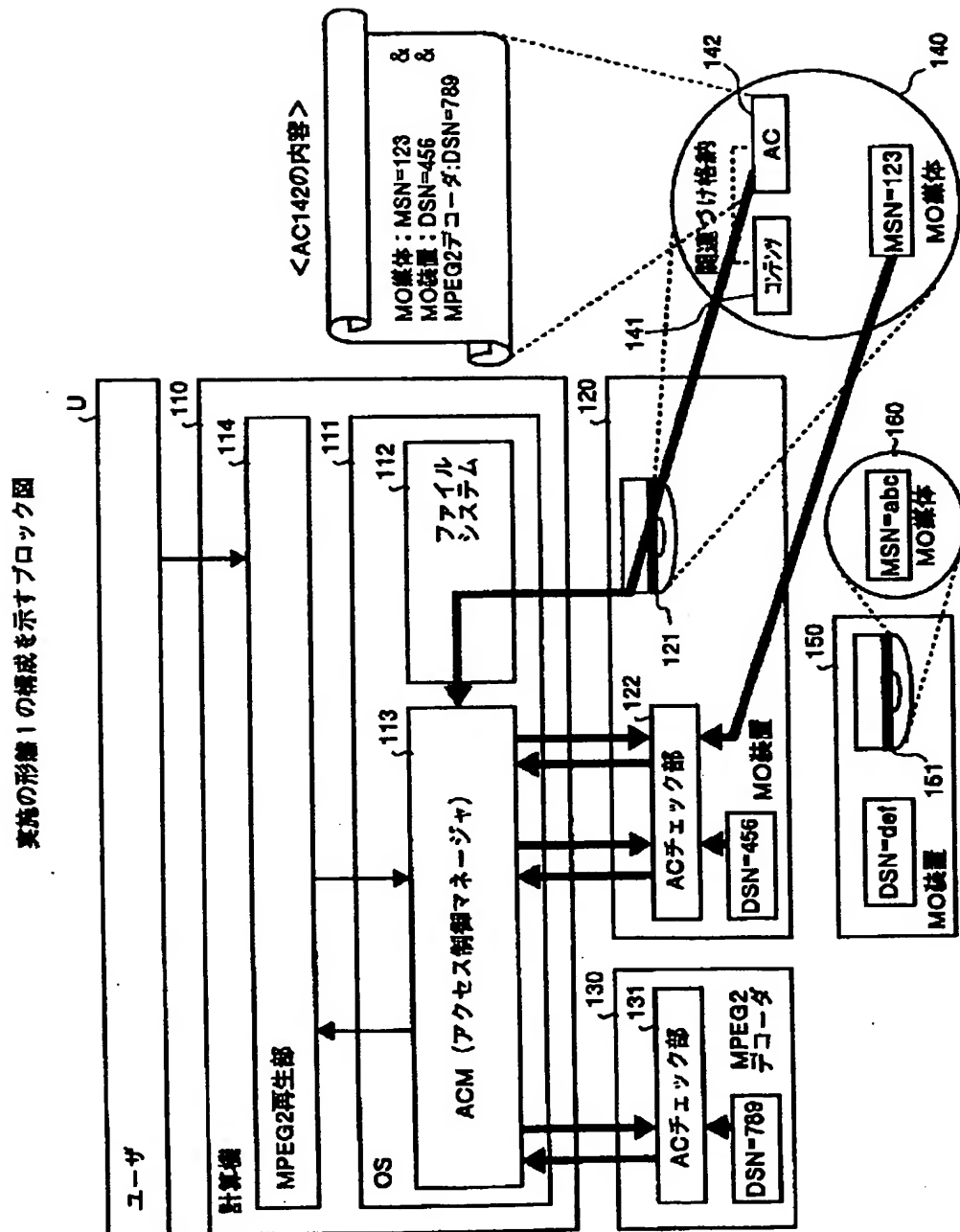


【図3】

図1に示したAC142のフォーマットの一例を示す図

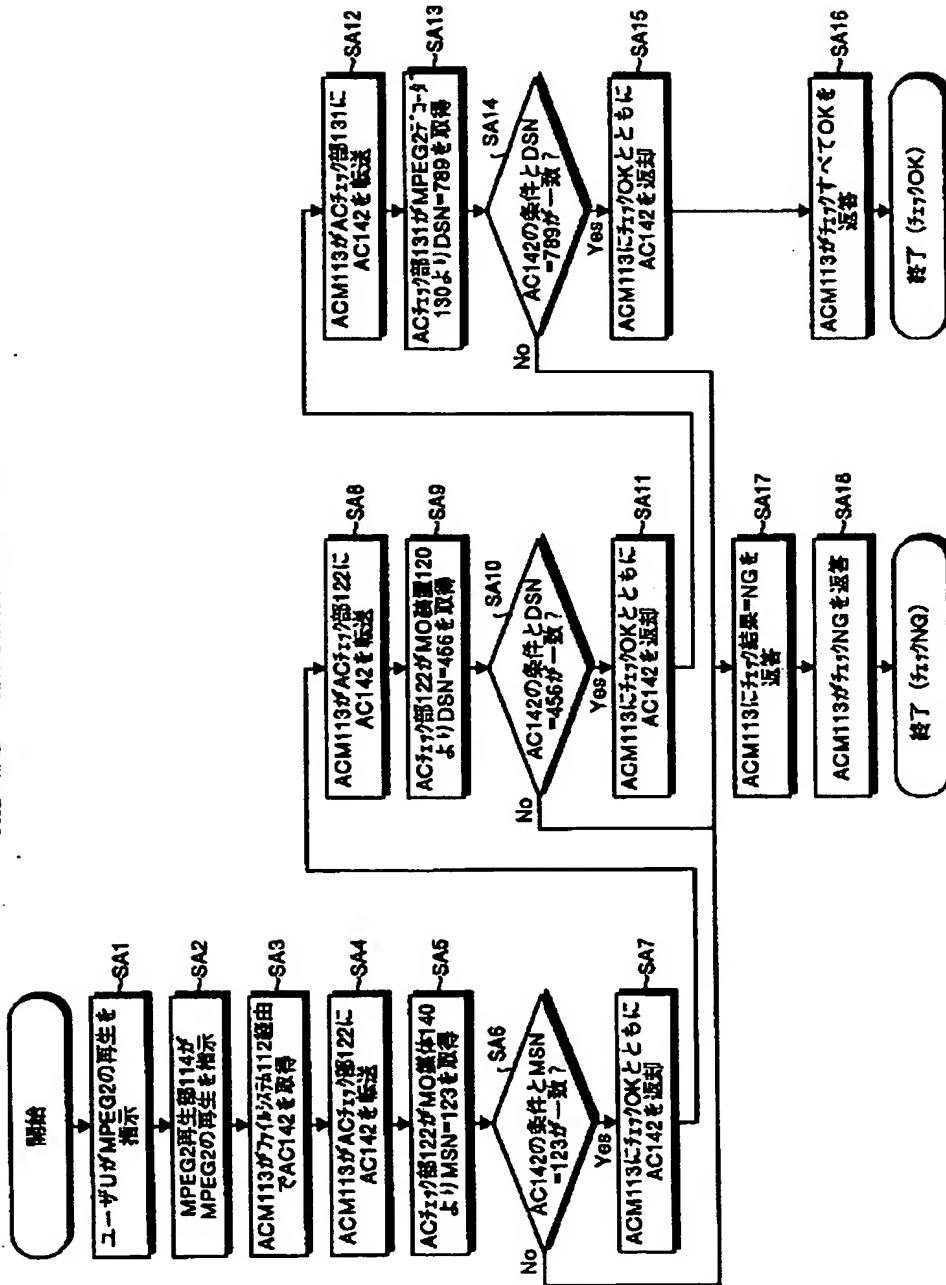


【図 1】

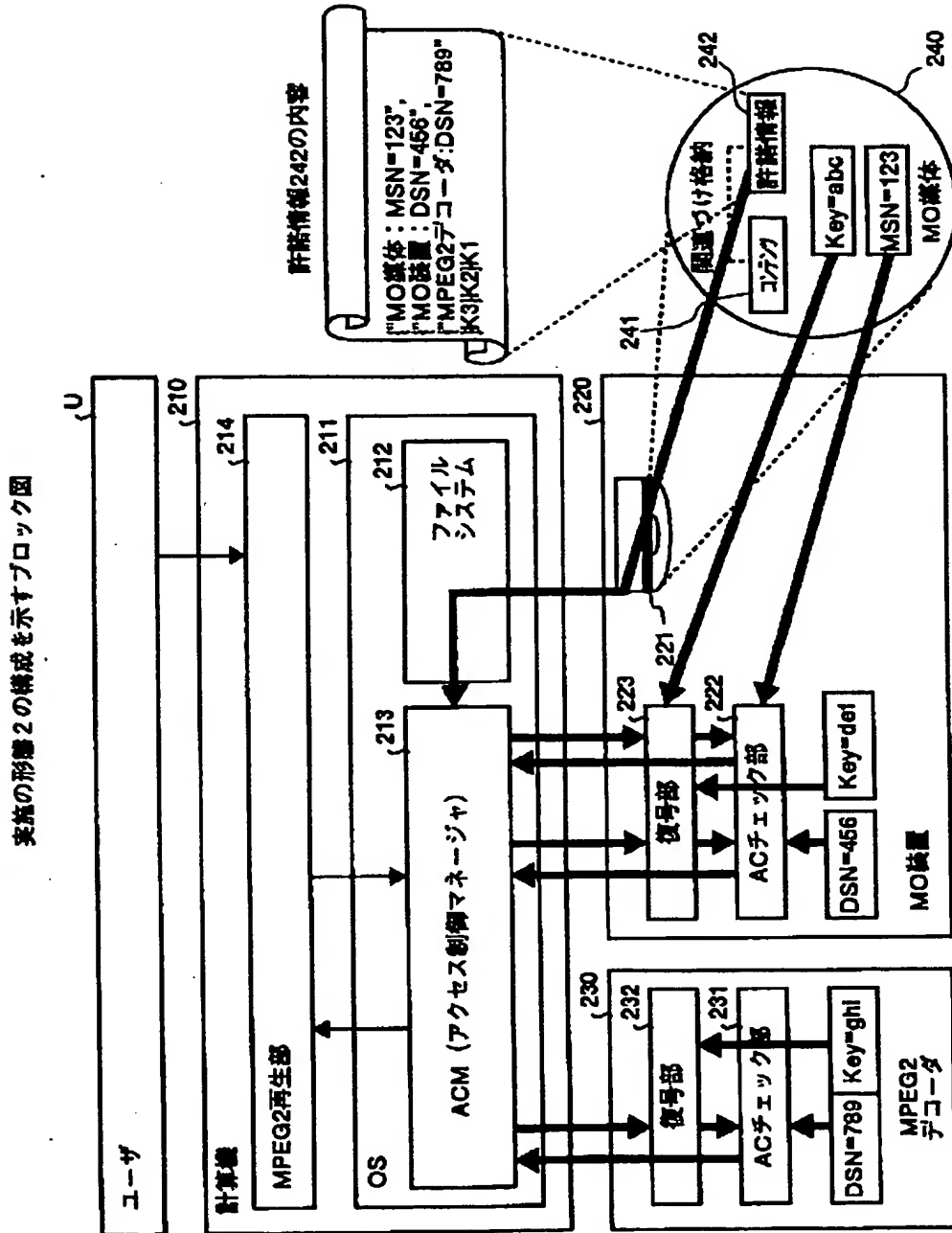


【図4】

実施の形態1の動作を説明するフローチャート

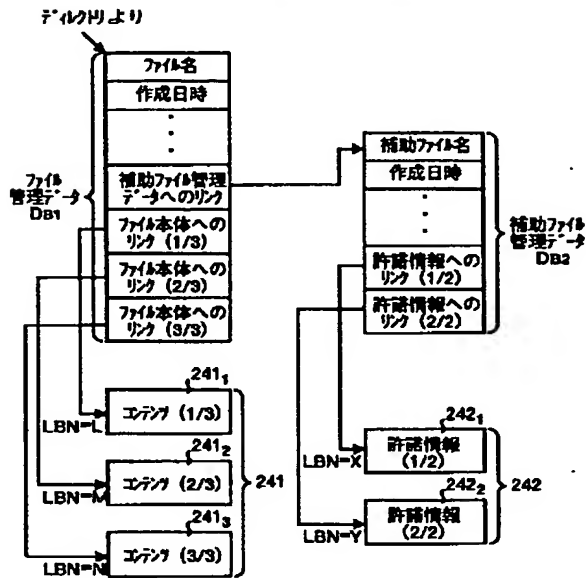


【図5】



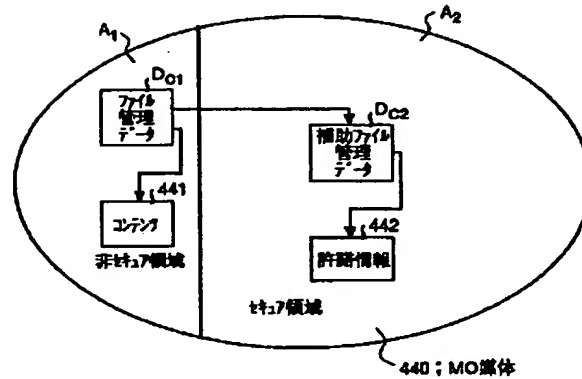
【図6】

図5に示したエンタ241と許諾情報242との関係を示す図



【図15】

図14に示したMO媒体440におけるデータ構造を示す図



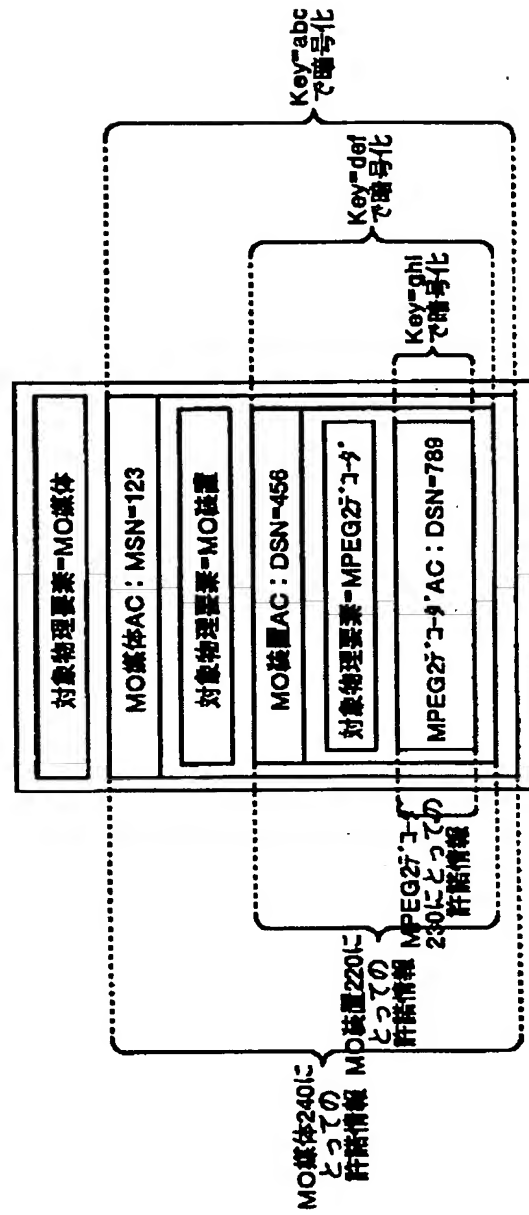
【図8】

図5に示した許諾情報242の一例を示す図

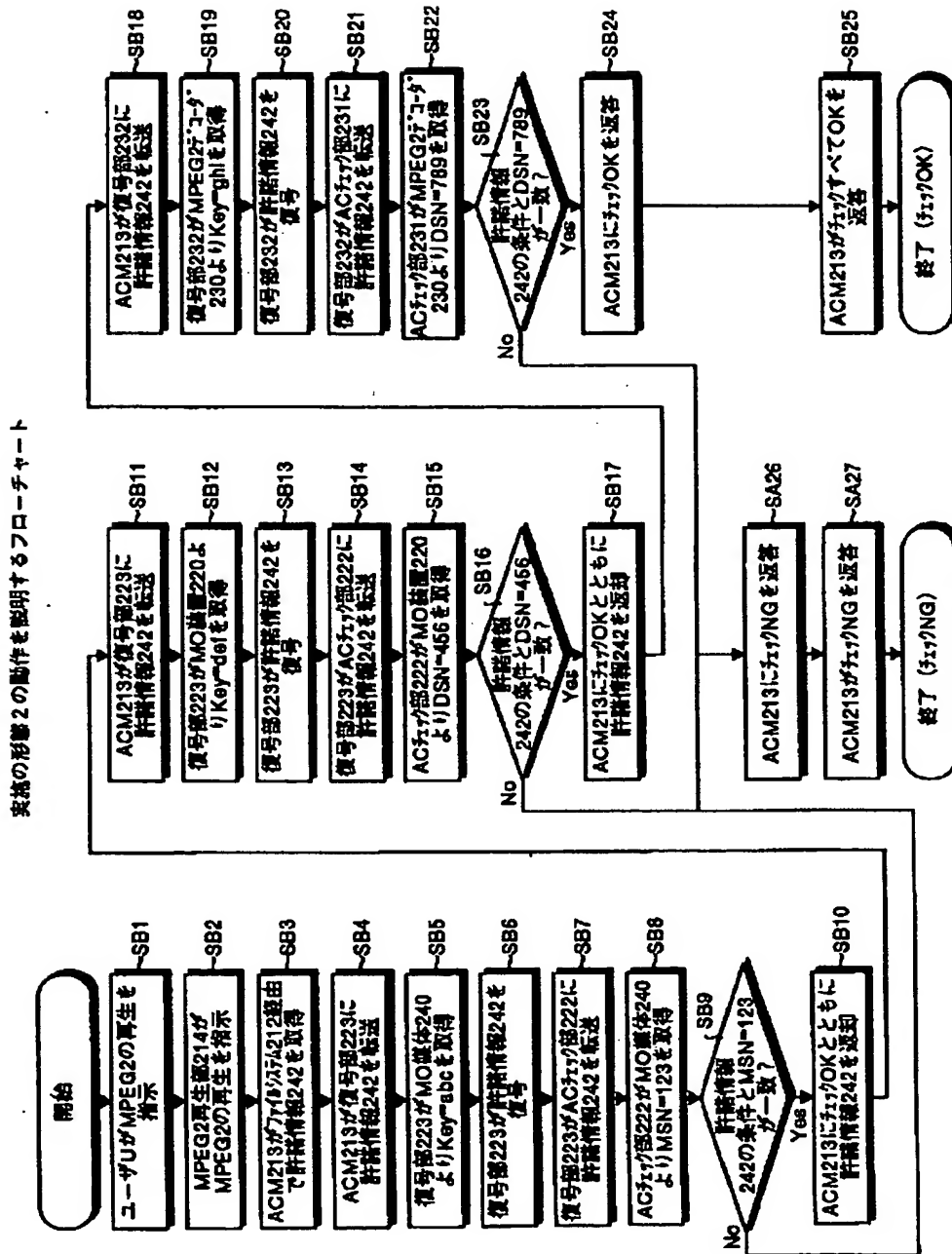
- (a) { "MO媒体: MSN=123", { "MO装置: DSN=456", { "MPEG2データ: DSN=789" } K3} K2} K1
- (b) "MO媒体: MSN=123", { "MO装置: DSN=456", { "MPEG2データ: DSN=789" } K3} K2
- (c) { "MO装置: DSN=456", { "MPEG2データ: DSN=789" } K3} K2
- (d) "MO装置: DSN=456", { "MPEG2データ: DSN=789" } K3
- (e) { "MPEG2データ: DSN=789" } K3
- (f) "MPEG2データ: DSN=789"

【図7】

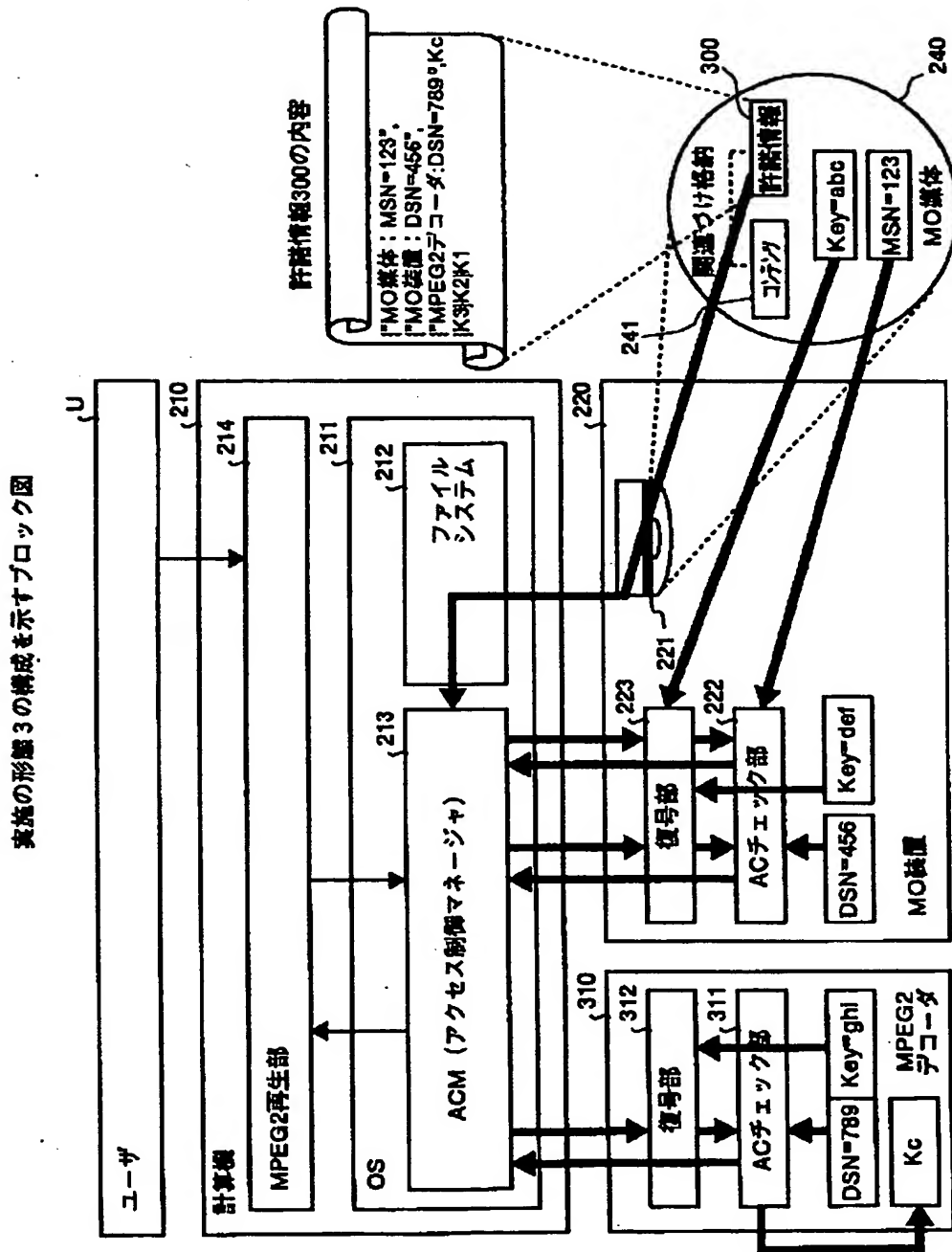
実施の形態2におけるライセンスの一例を示す図



【図9】

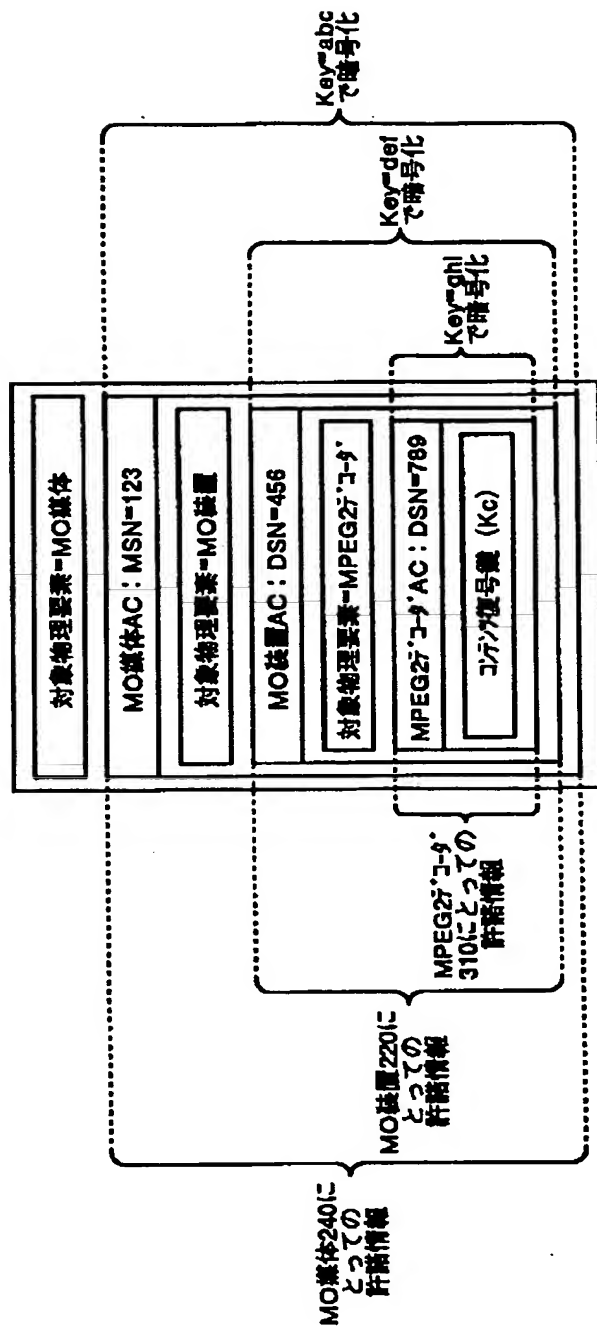


【図10】



【図11】

実施の形態3におけるラベルの一例を示す図



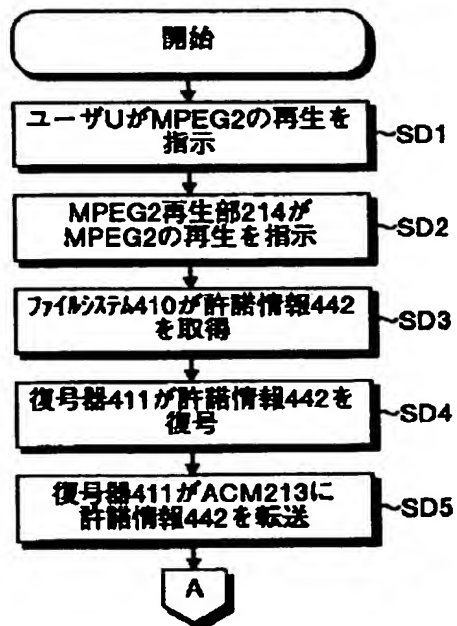
【図12】

図10に示した許諾情報300の一例を示す図

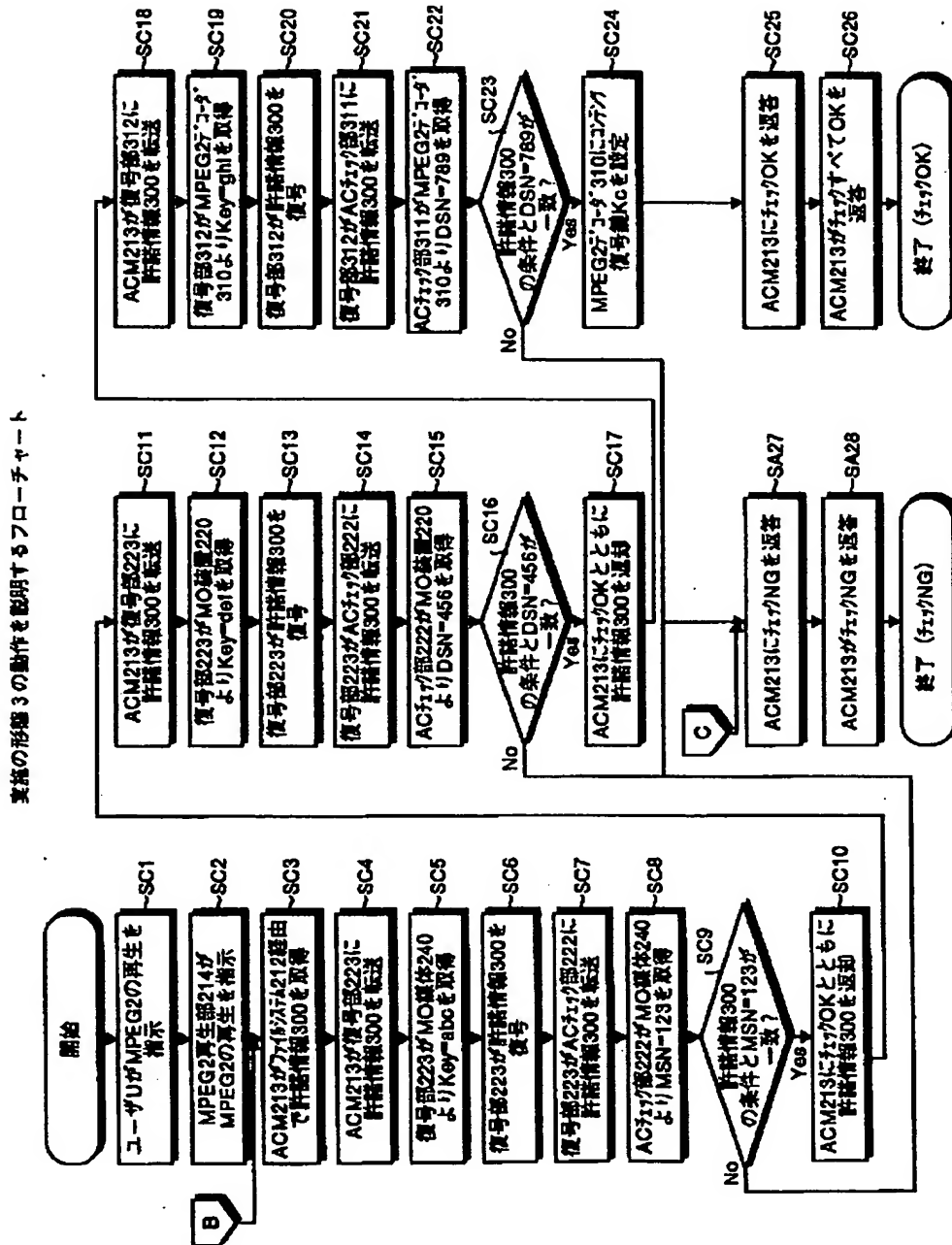
- (a) { "MO媒体: MSN=123" , { "MO装置: DSN=456" , { "MPEG2データ: DSN=789" ,Kc} K3} K2} K1
- (b) "MO媒体: MSN=123" , { "MO装置: DSN=456" , { "MPEG2データ: DSN=789" ,Kc} K3} K2
- (c) { "MO装置: DSN=456" , { "MPEG2データ: DSN=789" ,Kc} K3} K2
- (d) "MO装置: DSN=456" , { "MPEG2データ: DSN=789" ,Kc} K3
- (e) { "MPEG2データ: DSN=789" ,Kc} K3
- (f) "MPEG2データ: DSN=789" ,Kc

【図16】

実施の形態4の動作を説明するフローチャート

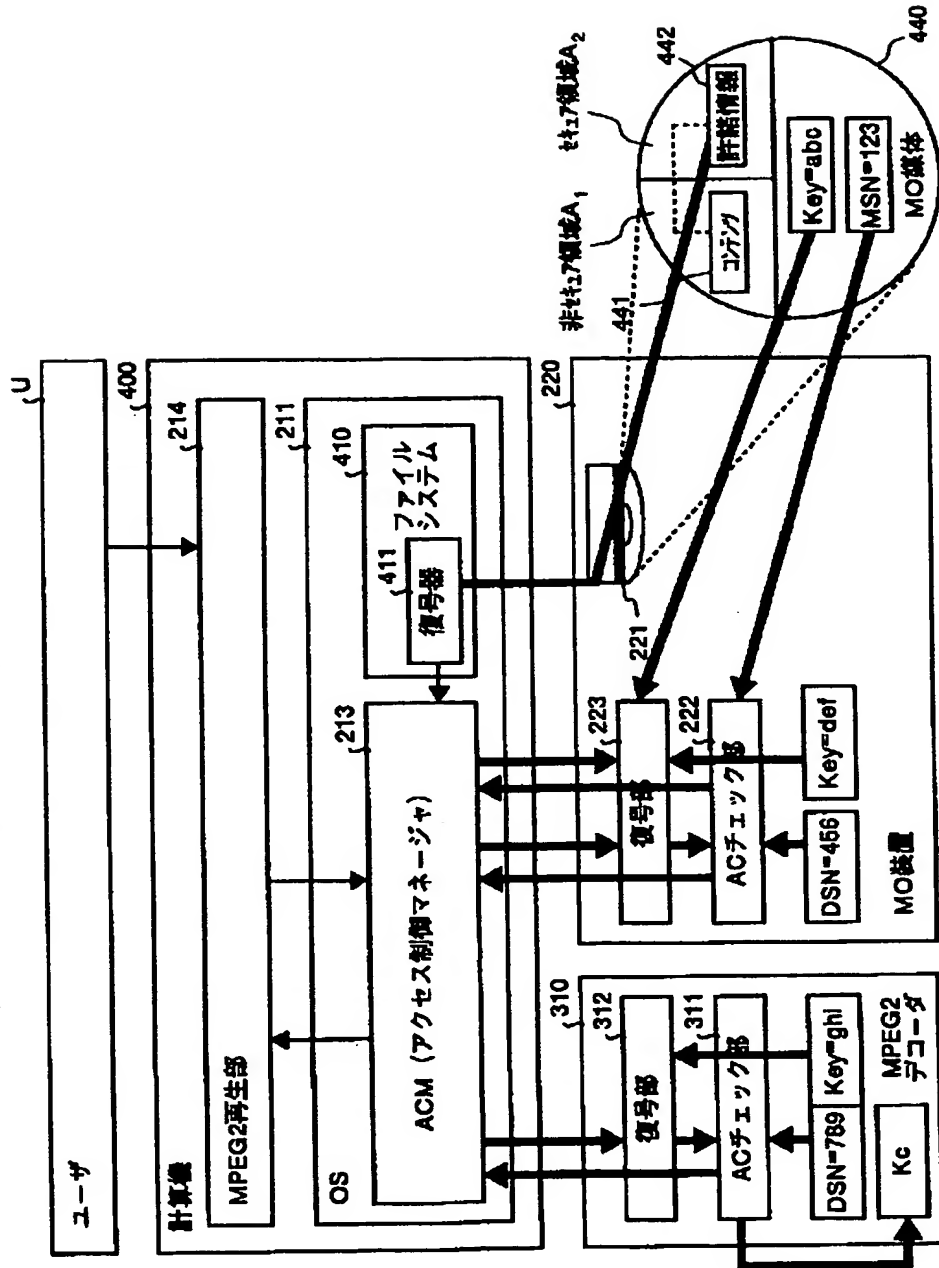


【図13】



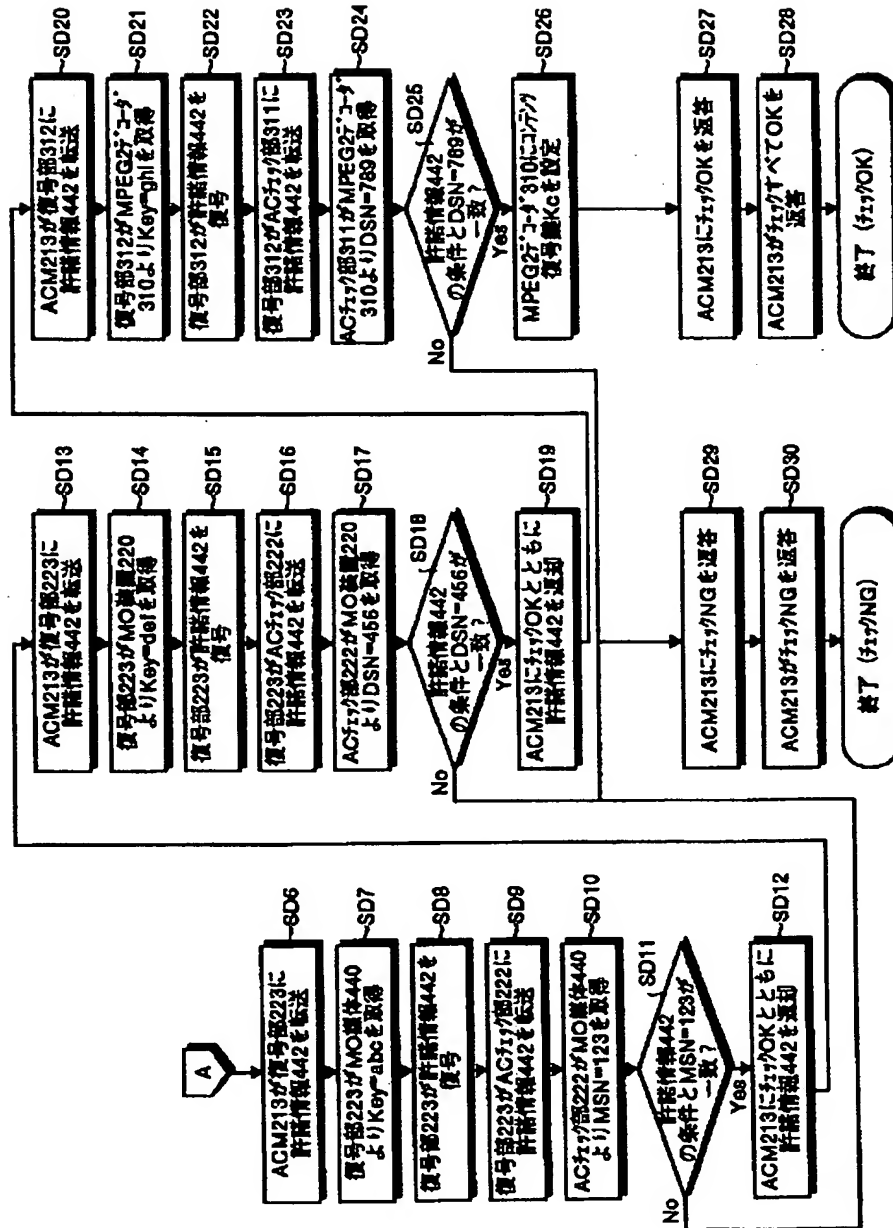
【図14】

実施の形態4の構成を示すブロック図

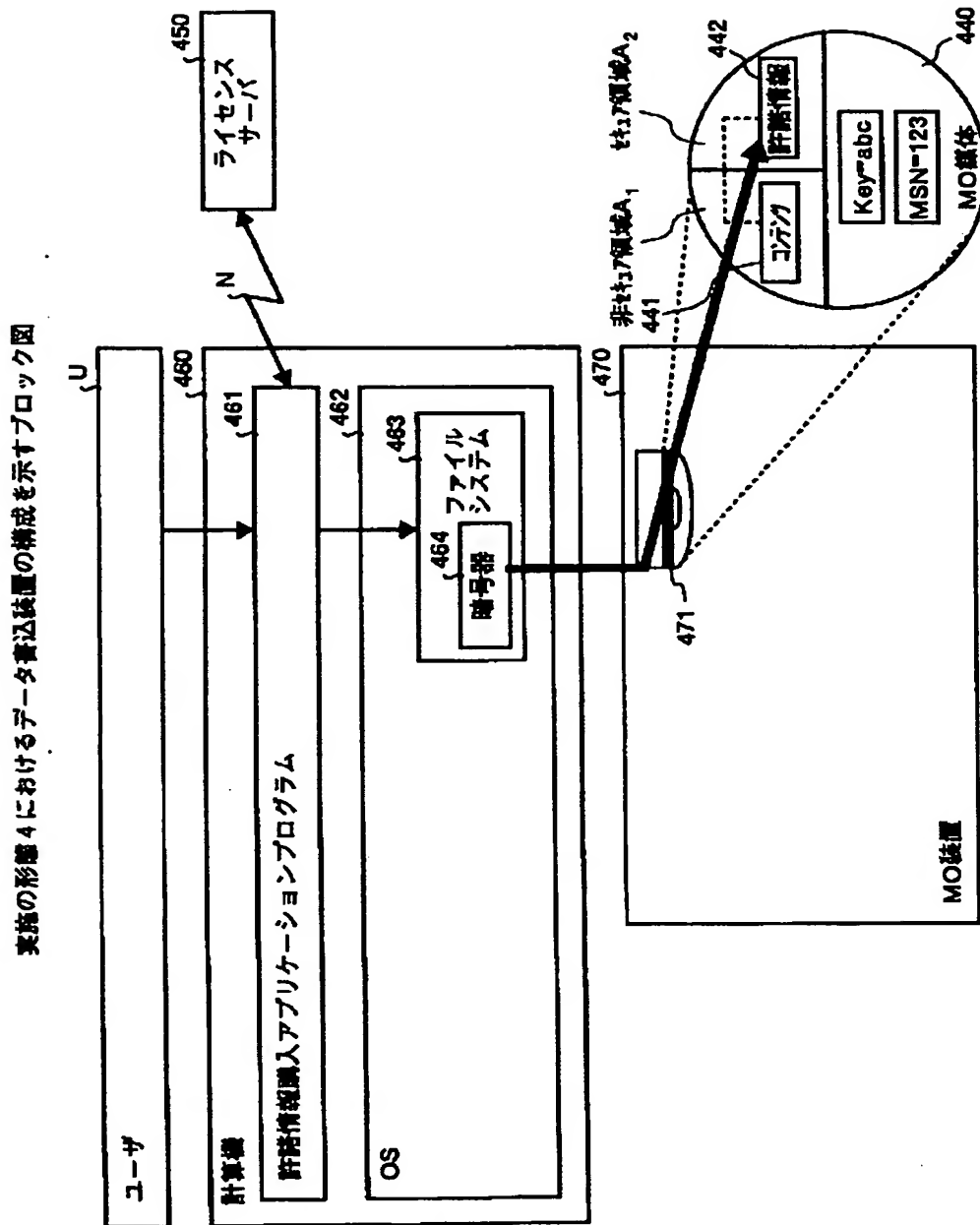


【図17】

実施の形態4の動作を説明するフローチャート

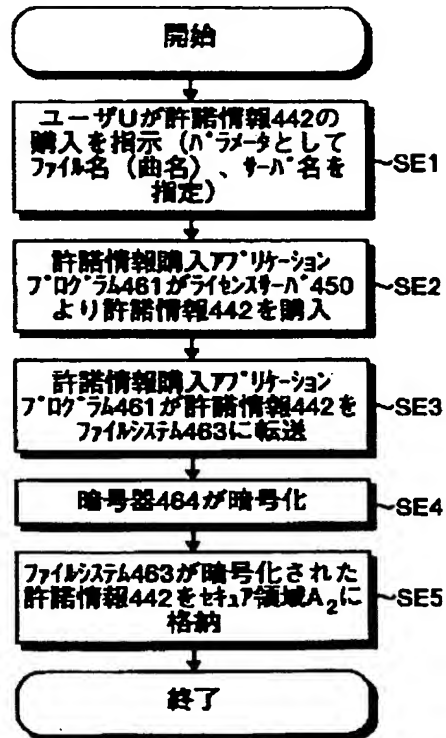


【図18】



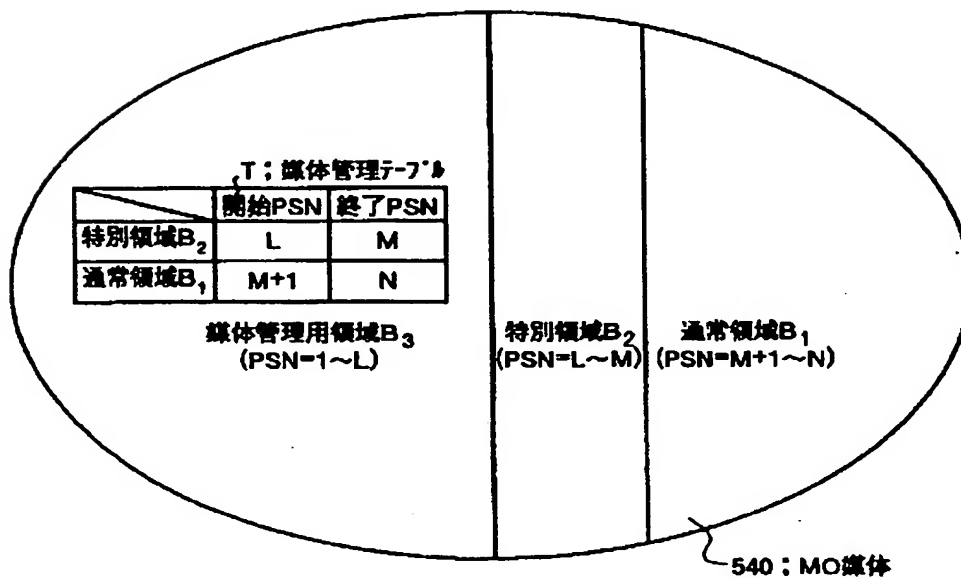
【図19】

図18に示したデータ書込装置の動作を説明するフローチャート



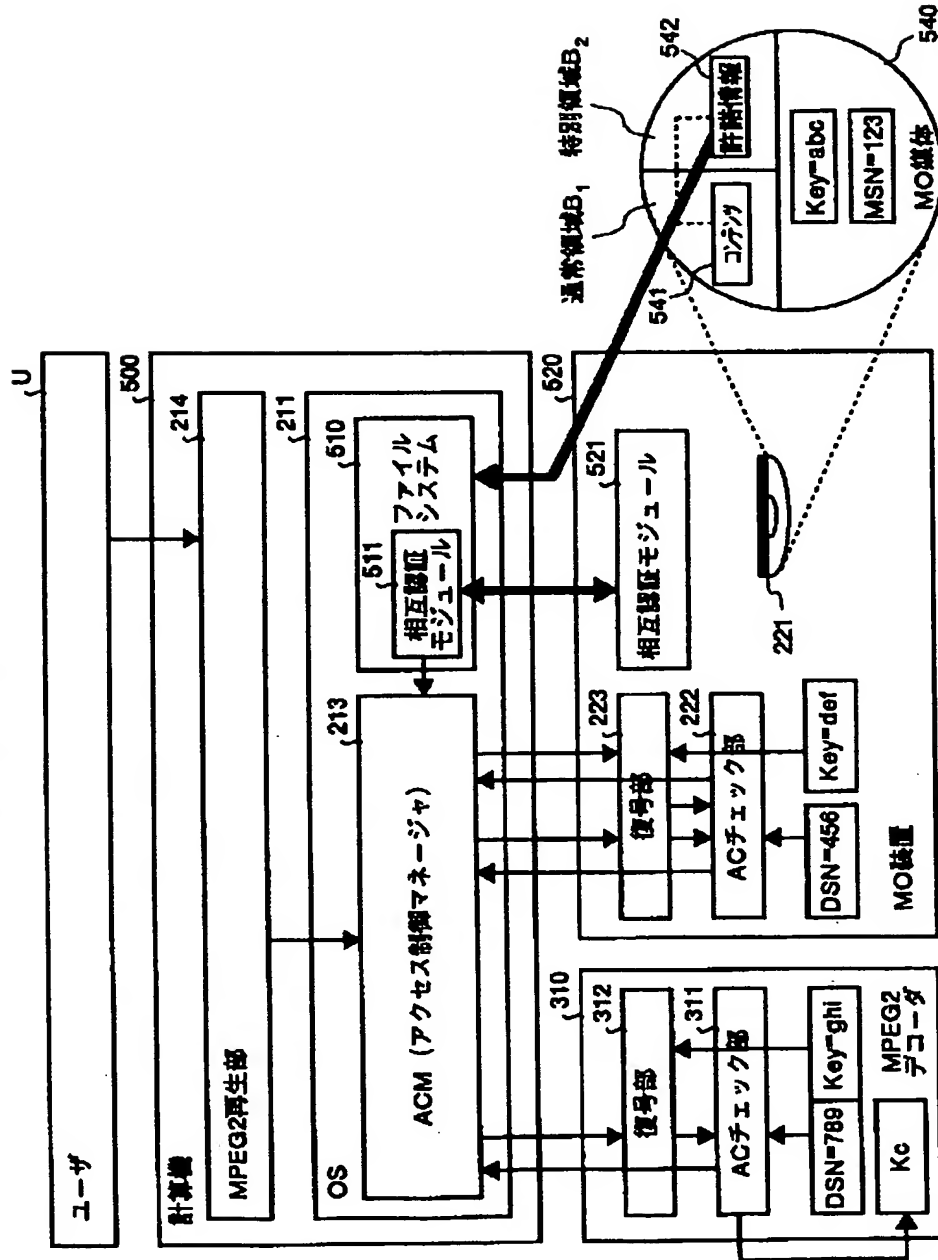
【図21】

図20に示したMO媒体540におけるデータ構造を示す図



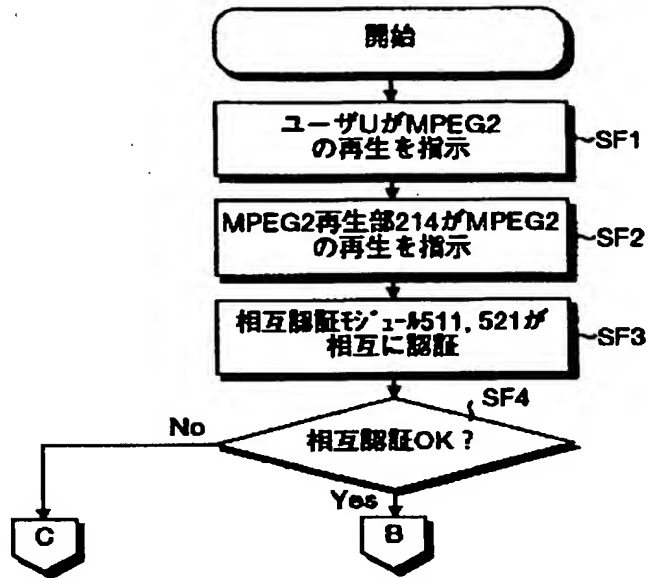
【図20】

実施の形態5の構成を示すブロック図



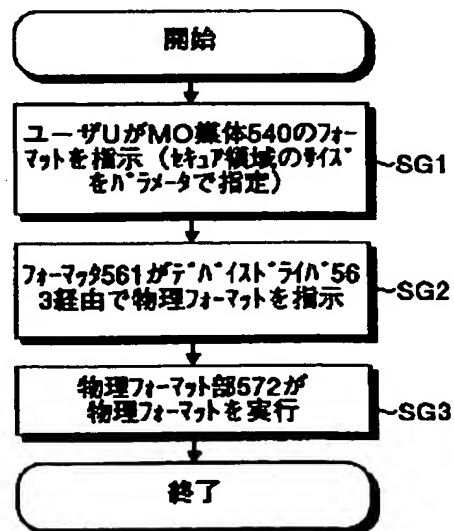
【図22】

実施の形態5の動作を説明するフローチャート



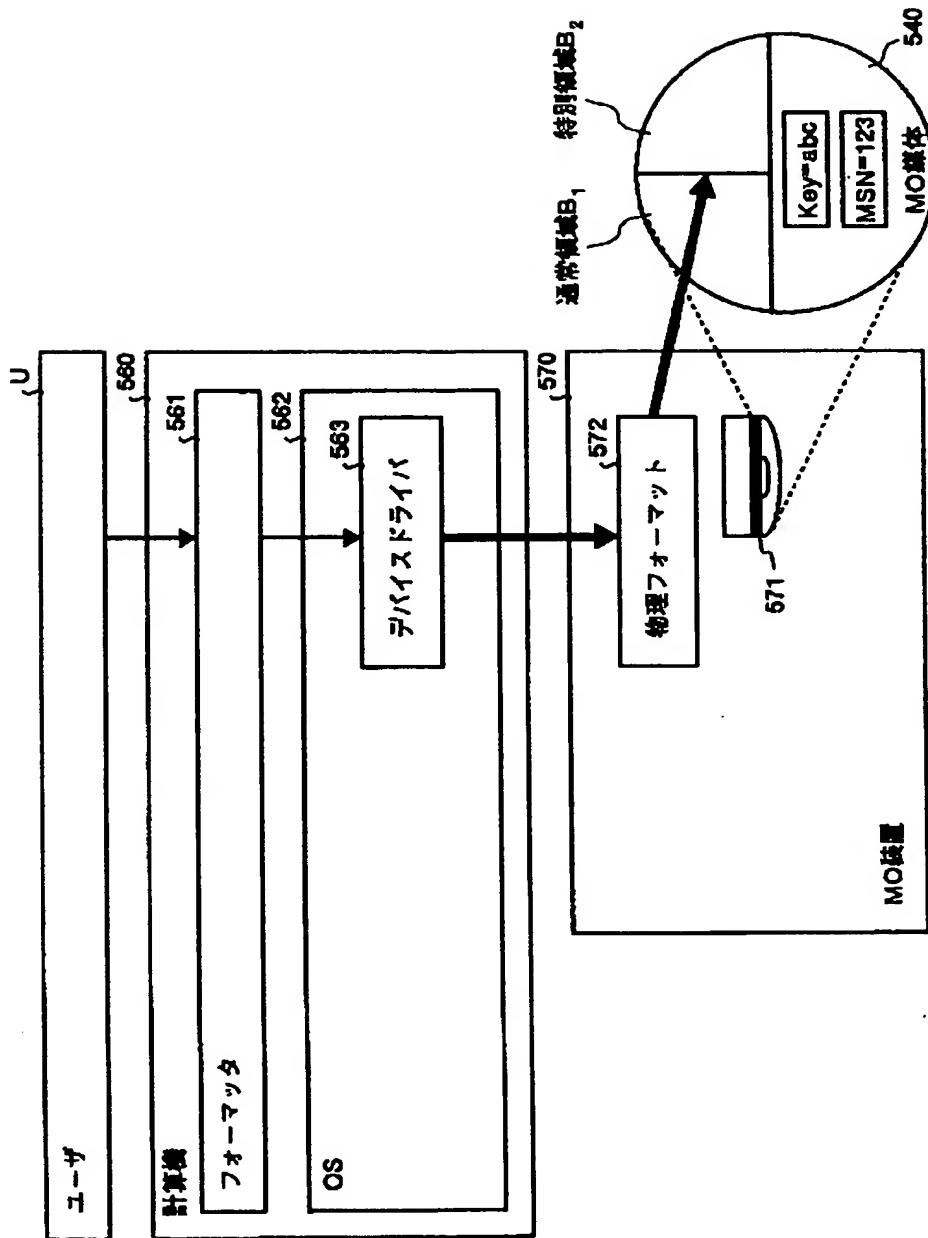
【図24】

図23に示したフォーマット装置の動作を説明するフローチャート



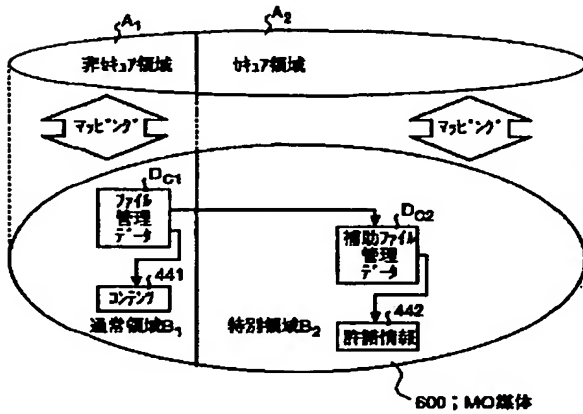
【図23】

実施の形態5におけるフォーマット装置の構成を示すブロック図



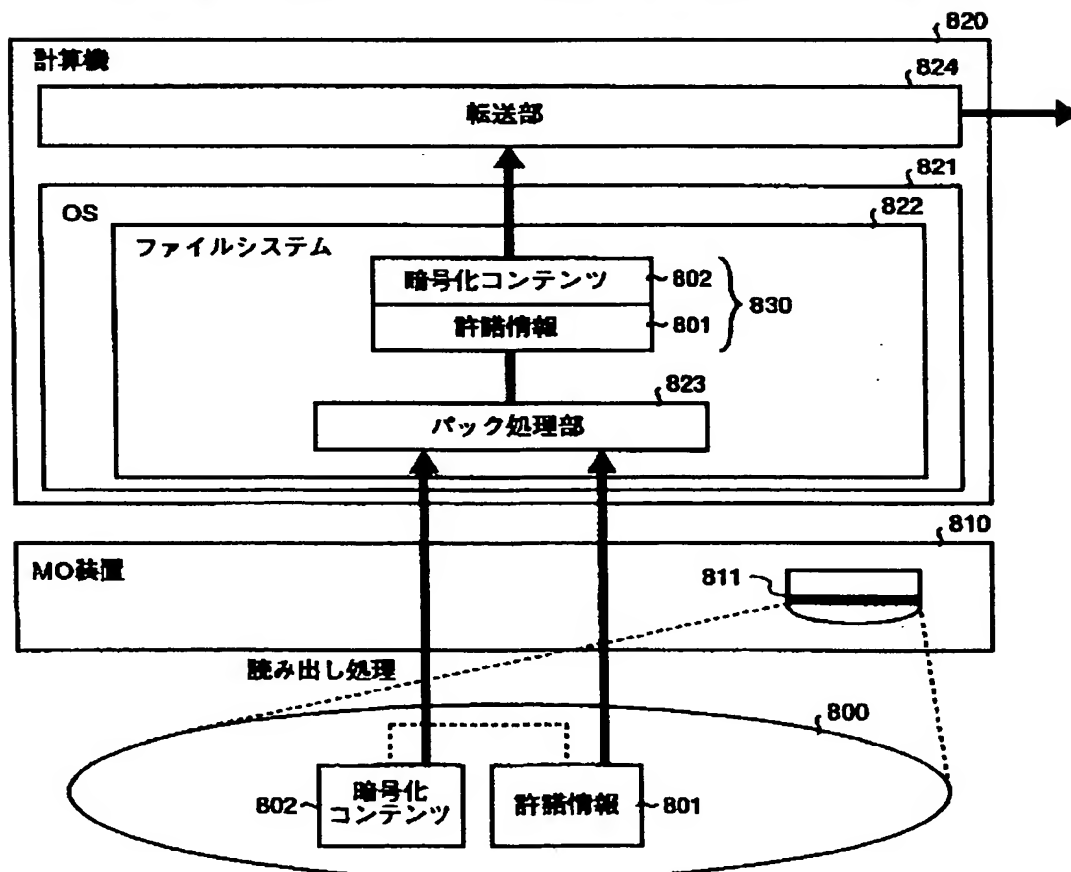
【図25】

実施の形態6におけるMO媒体600のデータ構造を説明する図



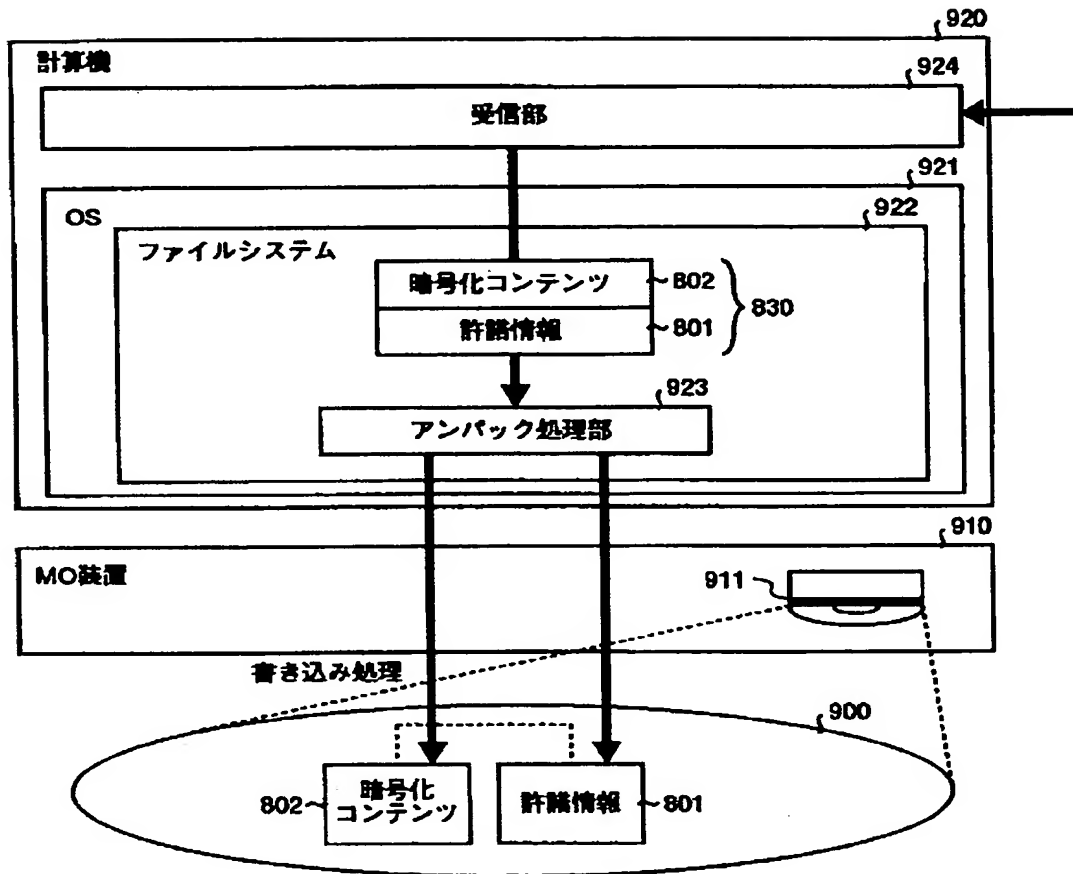
【図26】

実施の形態7におけるバックデータ生成装置の構成を示すブロック図



【図27】

実施の形態7におけるアンパック装置の構成を示すブロック図



フロントページの続き

(72)発明者 小野 越夫
神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

(72)発明者 畑中 正行
神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

(72)発明者 吉田 正敏
神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

(72)発明者 中井 孝博
神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

Fターム(参考) 5B017 AA07 BA05 BA07 BB02 BB10
CA09 CA15 CA16
5B049 AA01 AA05 BB11 CC05 EE05
EE28 GG04 GG07 GG10
5B089 GA21 JA33 JB24 KA17 KB13
KC58 KH30
9A001 EE03 LL03